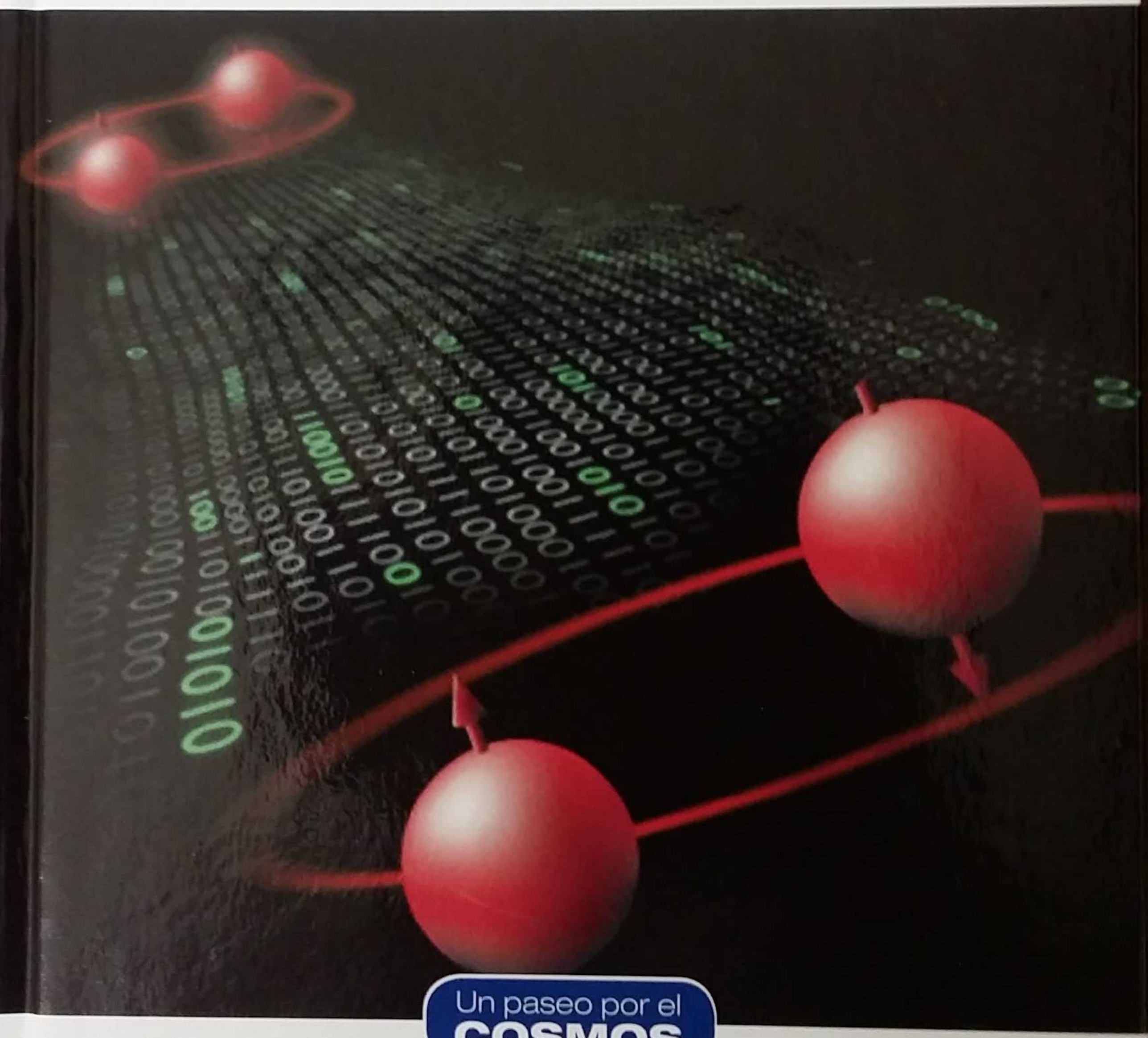
Computación, teleportación y criptografía cuánticas

La segunda revolución cuántica



Un paseo por el **COSMOS**

Computación, teleportación y criptografía cuánticas

La segunda revolución cuántica

RBA

Imagen de cubierta: Las nuevas tecnologías cuánticas de la información, que se basan en el procesado de los bits cuánticos o «qubits», capaces de ocupar estados que son superposición de varios de ellos y pueden presentar entrelazamiento, están configurando un desarrollo científico en el que fenómenos como el teletransporte y la computación cuántica son ya realidad.

Dirección científica de la colección: Manuel Lozano Leyva

Realización: EDITEC
Diseño cubierta: Llorenç Martí
Diseño interior: tactilestudio
Infografías: Joan Pejoan
Fotografías: J. Amini/NIST/Wikimedia Commons: 105; Archivo Federal de Alemania: 131ad; Archivo RBA: portada, 79a, 131ai; Jon Callas/Wikimedia Commons: 131b; D-Wave Systems, Inc.: 113a, 113b; P. Lameiro/Wikimedia Commons: 79b; Gunnar Ries/Wikimedia Commons: 25; Science Photo Library/Age Fotostock: 67a, 108-109; Frank Vincentz/Wikimedia Commons: 67b; Geoffrey Wheeler/NIST: 39.

ISBN: 978-84-473-8669-7
Depósito legal: B-8278-2017

Impreso y encuadernado en Rodesa, Villatuerta (Navarra)
Impreso en España - *Printed in Spain*

SUMARIO

INTRODUCCIÓN

Vivimos en un mundo hiperconectado, donde la información fluye desbordando todos los canales y saturando nuestros cerebros. Bajo ese caos aparente de inmensa trivialidad, subyacen, no obstante, autopistas de comunicación esenciales que vertebran la sociedad, de una manera tan fundamental que sin ellas, literalmente, se disolvería nuestro actual sistema de vida. Es imposible concebir una sociedad desarrollada sin una gestión adecuada de la información, tanto de su generación como de su preservación, transformación y transmisión. Las finanzas del mundo, la seguridad de las naciones, nuestra libertad, la paz y la guerra, nuestra salud, nuestra educación, nuestro ocio... no serían posibles si no estuviesen hoy por hoy configurados y trabados mediante un proceso continuo y digitalizado de información.

La física y la matemática, una pareja siempre inseparable, han sabido proporcionar durante los últimos siglos las herramientas que han permitido —y siguen permitiendo— esa eficaz gestión de la información. El nacimiento de la mecánica cuántica moderna, en la tercera década del siglo XX, vino a conferir un impulso esencial a esa tarea, haciendo posible la comprensión y el control de los materiales al descender a su interior más

profundo y pequeño. Pero aunque los revolucionarios transistores, por ejemplo, no existirían sin esa nueva física, en esencia el tratamiento de la información sigue siendo hoy en día ajeno a la cuántica, asentado en las leyes de la física clásica y regido por la teoría de la comunicación —también clásica— que desarrollaran Claude Shannon y Warren Weaver, a finales de la década de los cuarenta del siglo xx. Nuestros ordenadores domésticos, sin ir más lejos, no serían posibles sin el progreso que aportó la física cuántica, pero, aparte de eso (que no es poco), en su funcionamiento siguen siendo por completo clásicos. Calculan digitalizando la información en bits clásicos, y operan sobre ellos siguiendo las leyes de la teoría clásica de la información, sin que lo cuántico intervenga alterando esas reglas, al fin y al cabo las que rigen el macroscópico mundo que nos rodea.

Pues bien, parece que esa situación está cambiando, y que un futuro cuántico, también para la teoría de la información, está llamando a la puerta. Cuando empieza a cundir la idea de que «todo es cuántico», de que no se puede concebir que haya dos físicas separadas, una para nuestro cotidiano mundo macroscópico y otra para la profundidad de la materia, cuando lo cuántico empieza a emerger e imponer sus reglas a escalas de tamaño cada vez mayores, la información no podía quedar al margen. Se necesita entonces una nueva teoría de la información, cuántica, en el sentido de que aplique las leyes cuánticas en todas las etapas involucradas en la comunicación. Por ejemplo, sabemos que un modelo clásico involucra la emisión de un mensaje a partir de una fuente o emisor; su conversión en una señal; su cifrado, si se requiere preservar su confidencialidad; su transmisión eficaz por un canal, convenientemente protegido de ruidos y pérdidas; su recepción por el destinatario y su descodificación o lectura por el destinatario. Todas estas etapas se pueden cuantizar, lo que quiere decir que se pueden realizar utilizando recursos que conlleven que el proceso se rija de forma necesaria por las leyes cuánticas, tan profunda y conceptualmente distintas de las clásicas. La idea es explotar las posibles ventajas que aporten los nuevos métodos frente a los

tradicionales usados hasta ahora, ventajas que, obvio es, han de ser lo suficientemente importantes como para que compensen las desventajas de coste y complejidad que acarrean. Nacen así nuevos campos de investigación apasionantes y hoy en día punteros, como las tres aplicaciones cuánticas sobre las que trata este libro: la teleportación o transmisión de información a distancia sin que una señal recorra el camino intermedio; la computación por medio de máquinas que procesan información codificada sobre bits cuánticos —los *qubits*—, y la criptografía, que recurre a distribuir claves de cifrado cuya seguridad frente a la interceptación pivota sobre el indeterminismo cuántico.

Escribo estas líneas cuando acaba de hacerse público el premio Nobel de Física 2016, concedido a tres investigadores «por los descubrimientos teóricos de las transiciones de fase topológica y fases topológicas de la materia», que, se nos asevera, «contribuirán al desarrollo de la computación cuántica». Aquí lo tenemos, aunque de forma por ahora tangencial: la nueva teoría de la información cuántica, que incluye, entre otras, las tres aplicaciones antes nombradas, empieza a reconocerse como un campo de investigación fundamental, donde se está configurando la que será probablemente —con permiso de la biología, y también en conjunción con ella— la próxima revolución tecnológica. De la importancia que está cobrando dan una idea dos datos adicionales. Uno, que la agencia espacial china, el NSSC *(National Space Science Centre)*, esté desarrollando un programa de investigación, el QUESS *(Quantum Experiments at Space Scale)*, en cuyo marco lanzaron en el verano de 2016 un satélite dedicado a realizar experimentos de información cuántica, con el que se proponen, entre otros fines, estudiar el teletransporte a escala espacial. Y, segundo dato, que la Unión Europea esté considerando lanzar en 2018 el proyecto Quantum Flagship, dotado con unos mil millones de euros, para investigación en las nuevas tecnologías cuánticas de la información (específicamente, en computación cuántica). Es decir, con el mismo nivel de financiación que ha proporcionado a proyectos de investigación tan sonados e importantes como los dedicados a estudios sobre el grafeno y sobre el cerebro.

Acabamos esta breve introducción reproduciendo algunos párrafos del «manifiesto cuántico» que se ha lanzado, en el seno de las instituciones europeas, para promover una estrategia común en Europa para las investigaciones en este prometedor campo:

> Europa necesita invertir estratégicamente. Las tecnologías basadas en las leyes de la mecánica cuántica, que gobierna la física en la escala atómica, nos llevarán a una oleada de nuevas tecnologías que crearán nuevos negocios y nos ayudarán a resolver muchos de los desafíos globales actuales. A lo largo del último siglo, la humanidad ha logrado entender la física cuántica que subyace. Ahora, aspectos de la teoría cuántica que no habían sido aprovechados están listos para ser utilizados como recursos de nuevas tecnologías cuyas aplicaciones serán amplias y profundas, incluyendo redes de comunicaciones seguras, sensores de alta sensibilidad para la toma de imágenes en biomedicina y, fundamentalmente, nuevos paradigmas en computación. En cada una de estas aplicaciones, las tecnologías cuánticas podrían propiciar unas mejoras revolucionarias en términos de capacidad, sensibilidad y velocidad, y serán factores decisivos para el éxito en muchas industrias y mercados. Las aplicaciones tienen una importancia estratégica para la independencia de Europa y su seguridad, por ejemplo, en el campo del almacenaje y transmisión seguros de información, y en la creación de nuevos materiales para innovaciones en medicina y recursos energéticos. Los Gobiernos y las compañías de todo el mundo, incluyendo a Google, Microsoft, Intel, Toshiba e IBM, están realizando sustanciosas inversiones para liberar todo este potencial. Con el fin de que Europa permanezca a la vanguardia de esta tecnología emergente y participe en la industria cuántica global, necesita aumentar sus inversiones y hacer el mejor uso de su excelencia en ciencia e ingeniería, a fin de liderar la segunda revolución cuántica.

CAPÍTULO 1

Física para una teoría cuántica de la información

La física cuántica nos proporciona una nueva manera de mirar y comprender el mundo, y también de procesar y transmitir la *información*, que empieza a configurarse como un concepto fundamental para la indagación científica del universo. Y lo hace de una manera tan profunda que algunos hasta se atreven a postular que la realidad pudiera ser pura información.

La física cuántica ha contribuido de forma fundamental a configurar el tecnológico mundo desarrollado que nos rodea, en lo que se denominó la «revolución cuántica» del siglo xx. A punto de convertirse en centenaria, la teoría explora el campo de la información, derribando de nuevo algunos dogmas clásicos y anunciando lo que empieza a llamarse la segunda revolución cuántica. En este capítulo vamos a desarrollar unos fundamentos mínimos de física cuántica, imprescindibles para adentrarnos en ella.

CUANTIZANDO LA NATURALEZA

A lo largo del siglo xx, el esfuerzo de un nutrido grupo de científicos logró desarrollar la mecánica cuántica, un nuevo formalismo matemático que resultó ser la única teoría válida para el estudio de los fenómenos a escala microscópica, allí donde la física clásica fracasa. En su versión no relativista, el ingrediente esencial de la mecánica cuántica es la ecuación de Schrödinger, una ecuación cuya protagonista principal es la *función de*

onda, convencionalmente representada con la letra griega Ψ (psi). La ecuación, un histórico logro científico, nos permite resolver cómo evoluciona con el tiempo su solución, la función Ψ, y posee una característica destacable: relaciona números complejos, esto es, números que incorporan en su expresión la unidad imaginaria, i, o raíz cuadrada del número entero negativo –1 (su cuadrado toma el valor –1, o sea, $i^2=-1$). En general, la expresión de un número complejo z es de la forma $z=x+i\cdot y$, donde x e y son dos números reales; su módulo, $|z|$, se define como la cantidad cuyo cuadrado es $|z|^2=x^2+y^2$, un valor que es siempre un número real. Los números reales son los corrientes, los que usamos de forma habitual en nuestro día a día, y los que se emplean para expresar las cantidades de todas las magnitudes físicas, o propiedades medibles en los experimentos científicos. A diferencia de los complejos, los números reales pueden ser positivos o negativos; en particular, el módulo de un número complejo es siempre positivo. Los números complejos no cuantifican magnitudes observables (medibles) en nuestro mundo natural; no obstante, resultarán imprescindibles para la mecánica cuántica.

> Tenemos un esquema matemático consistente [...] Nada hay en la naturaleza que no pueda ser descrito por este esquema matemático.
>
> **Werner Heisenberg**

La ecuación de Schrödinger determina la evolución temporal de Ψ, también denominada *amplitud de probabilidad*, una función que, dada la característica ya señalada de la ecuación de la que es solución, es en general compleja, es decir, toma valores que son números complejos. Esto nos hace comprender que Ψ, la función de onda solución de la ecuación, no puede ella misma cuantificar de forma directa ninguna magnitud física o propiedad observable en nuestro mundo natural. ¿Cuál es entonces su interpretación? En 1926, Max Born desarrolló la que se conoce como la interpretación probabilística de la función de onda, que la considera como una amplitud de probabilidad, a partir de la cual, de modo general, se puede obtener la distribución estadística teórica esperable para los resultados experimentales de la medida de cualquier propiedad física —un *observable*— del

sistema, cuando este ocupa el estado físico correspondiente o descrito por esa función de onda particular Ψ.

La ecuación de Schrödinger, postulada en 1926, disolvió la clásica pregunta «¿lo que interviene en este fenómeno es una onda o un corpúsculo?», sustituyéndola por una respuesta rotunda: cada fenómeno observado se justifica mediante unas funciones matemáticas Ψ, o amplitudes de probabilidad que, sin ser ondas reales, también pueden interferir entre sí, reforzándose o cancelándose, de forma lejanamente análoga a como lo hacen las ondas reales clásicas (es por esto por lo que, a veces, luz más luz produce oscuridad). Además, posee otra característica esencial: su forma matemática hace que, dadas dos de sus soluciones, Ψ_1 y Ψ_2, asociadas a dos estados posibles 1 y 2 del correspondiente sistema físico, la suma o *superposición* general $a\cdot\Psi_1+b\cdot\Psi_2$, donde a y b son dos números (en general complejos), constituye otra solución de la ecuación. Es decir, la superposición de dos estados de un sistema cuántico representa, en general, otro estado en el que el correspondiente sistema físico se puede, en principio, «situar» (una forma de decir que esa función de onda es la descripción teórica adecuada para ese sistema, en cada instante). Este resultado va a ser crucial en la nueva teoría, y el responsable en gran medida de que la descripción cuántica de los fenómenos se aparte de forma radical del modo de descripción que realiza la física clásica.

Conocida la función de onda en un instante de tiempo dado, la ecuación de Schrödinger proporciona de forma determinista su evolución temporal, marcando, pues, cómo evolucionan las distribuciones de probabilidad de los resultados de los posibles experimentos sobre el sistema, es decir, fijando todo estado suyo futuro o pasado, siempre que en su evolución dicho sistema no experimente interacciones. Por el contrario, si no se da ese aislamiento, el azar se cuela en la teoría y el determinismo desaparece: el formalismo cuántico establece también como axioma la *reducción* o *colapso* de la función de onda. Este colapso consiste en que el sistema, debido a cualquier interacción que sufra, como la que conlleva un experimento de medida de cualquiera de sus propiedades, cambia de estado de una forma brusca y

azarosa, lo que matemáticamente se expresa como una modificación «instantánea», o colapso, de la función de onda que describe el sistema.

Veamos un ejemplo de cómo en física cuántica se utilizan las funciones de onda superpuestas para elaborar una descripción que no es determinista, es decir, deja que el azar decida, en general, cuál será el resultado específico de cada evento individual, de entre un conjunto de varios posibles. Se trata del famoso fenómeno cuántico denominado *efecto túnel*, constatado experimentalmente en innumerables ocasiones y según el cual existe una probabilidad apreciable de que una partícula atraviese una barrera de energía que, en términos clásicos, debería serle infranqueable, por faltarle energía para poder «saltarla». Por ejemplo, si consideramos un electrón que se aproxima a una barrera de potencial eléctrico cuya altura energética es mayor que la energía que trae él, en la descripción cuántica la función de onda Ψ toma valores no nulos también al otro lado de la barrera, luego la predicción teórica es que puede ocurrir que la partícula sea, en algunos casos, transmitida a través de la barrera, es decir, pueda acabar siendo localizada al otro lado de la misma.

Hasta que no se realice una observación, un experimento de localización o medida de la posición del electrón, el fenómeno viene descrito por una función de onda Ψ que representa un estado de superposición cuántica de dos posibilidades: que el electrón haya atravesado la barrera y que no lo haya hecho, como se muestra en la figura 1. Podemos simbolizar esta función como la suma:

$$\Psi = R \cdot \Psi_R + T \cdot \Psi_T$$

donde Ψ_R describe el estado cuántico de la partícula reflejada por la barrera, mientras que Ψ_T describe el estado de la partícula transmitida, al otro lado de la barrera. Los cuadrados de los módulos de los respectivos coeficientes numéricos R y T con que aparecen estas dos funciones de onda en la suma anterior proporcionan, de acuerdo con la interpretación probabilística, dos probabilidades: la de que el electrón se refleje en la barrera

FIG. 1

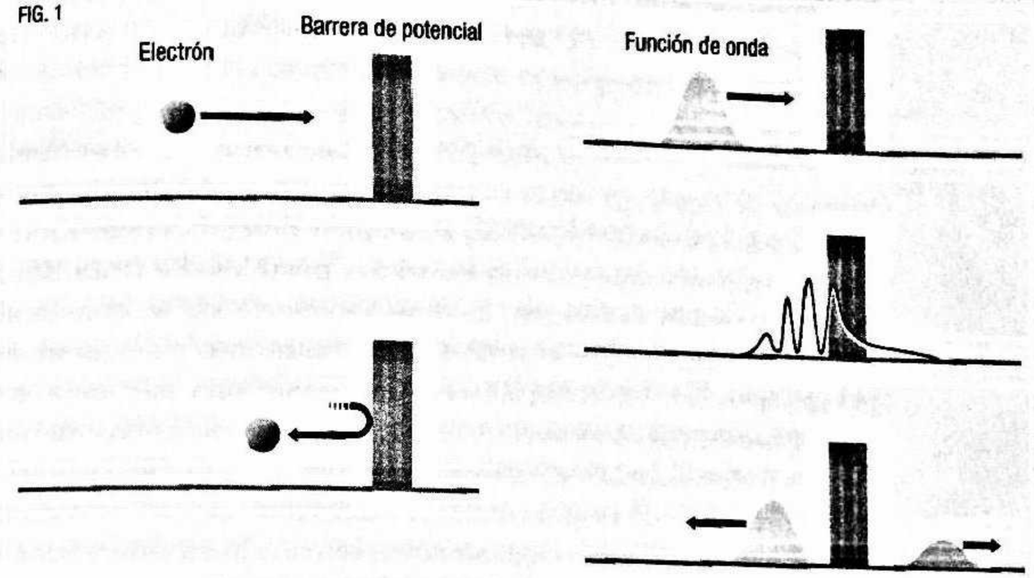


IMAGEN CLÁSICA
En física clásica, una barrera de potencial es infranqueable para una partícula que incide con una energía inferior a la altura energética de la barrera.

IMAGEN CUÁNTICA
En física cuántica, el electrón tiene una probabilidad no nula de pasar al otro lado de una barrera de potencial que debería repelerlo clásicamente.

Efecto túnel cuántico. Un objeto cuántico, como un electrón o una partícula alfa (un núcleo de helio, compuesto por dos protones y dos neutrones), que incide con determinada energía contra una barrera de potencial de altura superior a esa energía, puede atravesarla, algo imposible según la física clásica. Es un fenómeno estadístico: la probabilidad de que suceda es distinta de cero y lo que hará cada partícula concreta depende del azar.

($|R|^2$) y la de que ese mismo electrón la atraviese ($|T|^2$); la normalización de la probabilidad exigirá, por tanto, que la suma de $|R|^2$ y $|T|^2$ sea igual a 1. Es decir, la suma de las partículas reflejadas y transmitidas ha de ser igual al número de las incidentes, de forma que $100 \cdot |R|^2$ y $100 \cdot |T|^2$ representan los porcentajes respectivos de partículas reflejadas y transmitidas. El azar va a decidir si cada partícula individual, de un conjunto de muchas de ellas que inciden con igual energía, inferior a la necesaria clásicamente para que haya transmisión, atravesará la barrera o no. La estadística final del proceso, cuando se haya observado qué ha sucedido con muchos electrones incidentes con esa misma energía, es exactamente la predicha por la función de onda Ψ del sistema:

un porcentaje del $100 \cdot |R|^2$% de los electrones se habrán reflejado y un $100 \cdot |T|^2$% de ellos se habrán transmitido.

LA LUZ: ONDAS ELECTROMAGNÉTICAS Y CUANTOS DE ENERGÍA

En el siglo XIX James Maxwell estableció que la luz, esto es, cualquier radiación no constituida por partículas materiales, estaba compuesta por ondas electromagnéticas, es decir, que es una perturbación del campo electromagnético que se propaga por el espacio. En física, el término *campo* refiere a la situación en que, en una región dada del espacio, está presente una magnitud física, es decir, esa magnitud tiene un valor determinado en cada localización en la región y en cada instante. En particular, en una zona del espacio existe un campo electromagnético en un instante temporal dado cuando, en ese momento, están definidas en cada punto de esa región dos magnitudes físicas vectoriales: el campo eléctrico y el campo magnético. Recordemos que una magnitud física vectorial es aquella que requiere para su especificación completa de tres números reales, por ejemplo, módulo o valor absoluto, dirección y sentido. Convencionalmente, se suelen representar como flechas y el ejemplo típico es la velocidad: no basta con decir que nos movemos a tantos kilómetros por hora (rapidez o módulo $v = |\vec{v}|$ del vector velocidad $\vec{v}$), hay que añadir sobre qué dirección (por qué carretera nos movemos) y en qué sentido lo hacemos (de los dos posibles).

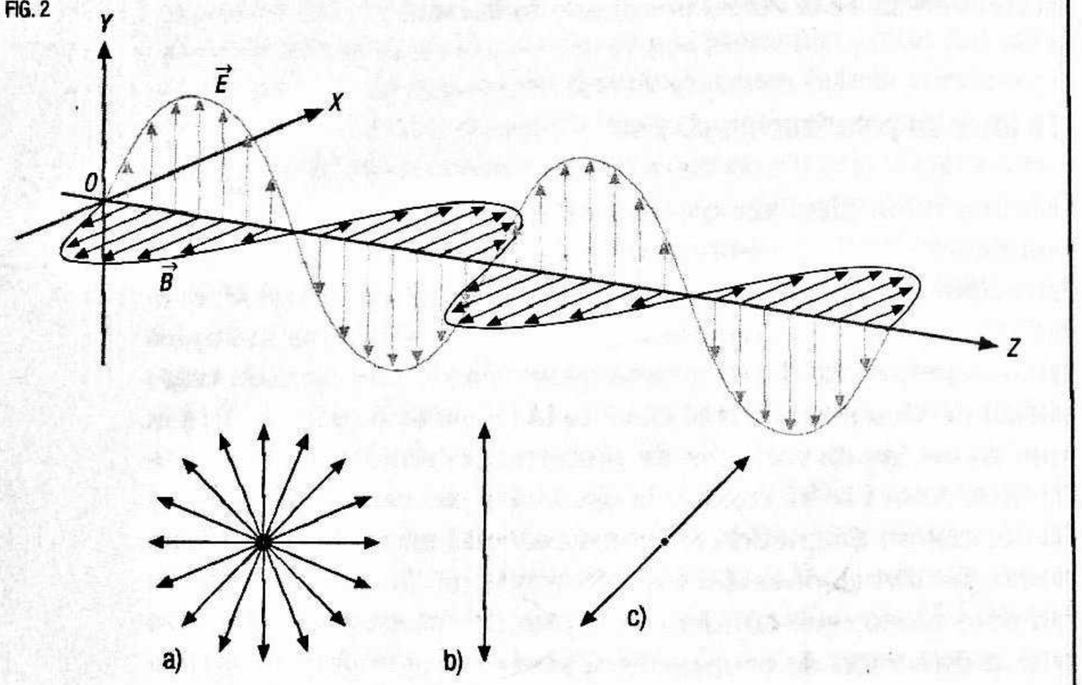
Maxwell, por tanto, concibió la luz como la propagación de una onda electromagnética: un campo eléctrico variable genera un campo magnético variable, y viceversa, y la propagación conjunta de sus variaciones por una región constituye un fenómeno ondulatorio continuo, capaz de avanzar por el vacío con la rapidez c = 299 972 km/s, transportando energía y sin necesidad de sustentarse en ningún medio material. El éxito de la concepción ondulatoria de la radiación fue apabullante, pero en 1905 Albert Einstein propuso una descripción teórica alternativa, postulando la discretización o cuantización de la luz. Con ello logró explicar de forma completa (algo que la teoría continua de Maxwell no permitía) el *efecto fotoeléctrico*, un fenómeno en el que, al iluminar un metal con luz ultravioleta, se produce la emisión de electrones. En concreto, Einstein conceptualizó la radiación como compuesta por paquetes indivisibles de energía, los «cuantos de luz», que fueron supuestos desplazándose en el espacio de forma localizada y con rapidez en el vacío igual a c. El popular nombre de *fotón* que se impuso a partir de 1926 para los cuantos de luz no autoriza, sin embargo, a concebirlos como «partículas» en el sentido usual o material, pues carecen de masa en reposo. La energía de cada cuanto viene dada por $E = h\nu$, donde h es la constante de Planck, de valor $h = 6{,}626069 \cdot 10^{-34}$ J·s, que en el año en que Einstein publicó su hipótesis cuántica acababa de aparecer en la historia, en el contexto de la explicación teórica de Planck para la radiación del cuerpo negro (1900); ν simboliza la frecuencia de la correspondiente radiación.

La luz y su polarización clásica

En una onda electromagnética clásica, los campos eléctrico y magnético oscilan, manteniéndose siempre perpendiculares a la dirección de propagación y entre sí (se trata de lo que se define como una onda transversal) y vibrando según los múltiples planos perpendiculares a cada dirección de propagación (algo difícil de visualizar). Es el caso de la luz solar o natural, para la que todas las direcciones de propagación son igualmente probables. Ahora bien, cuando la oscilación del campo eléctrico (y la del campo magnético, en consecuencia) no se produce según todas las direcciones del espacio, sino que queda contenida en un solo plano, que contiene siempre al vector campo eléctrico y a la dirección de propagación, se dice que la correspondiente onda electromagnética está linealmente polarizada. En la figura 2, arriba, se representa este caso; en particular, una onda transversal «plana», lo que quiere decir que los vectores campo eléctrico y campo magnético —las flechas en la figura— oscilan manteniéndose paralelos a sendas rectas fijas en el espacio; el plano que contiene el vector campo eléctrico y la dirección de

propagación se define por convención como el *plano de polarización*. En particular, se define la polarización lineal a un ángulo dado de θ grados cuando el vector campo eléctrico, visto de frente acercándose la onda según el eje Z de un sistema de tres ejes coordenados mutuamente perpendiculares, oscila al avanzar la onda de forma que su extremo se mueve según una línea recta que forma con el eje vertical de ese sistema de referencia un ángulo θ. En este caso, los términos específicos polarización «horizontal» y «vertical» se asocian, respectivamente, con los valores 90° y 0° (siempre referidos a los ejes coordenados que se hayan elegido). La onda representada arriba en la figura 2 se corresponde con el caso de polarización vertical, $\theta = 0°$; en la figura 3, arriba, se representa un caso de polarización lineal en diagonal, correspondiente a un ángulo de 45°.

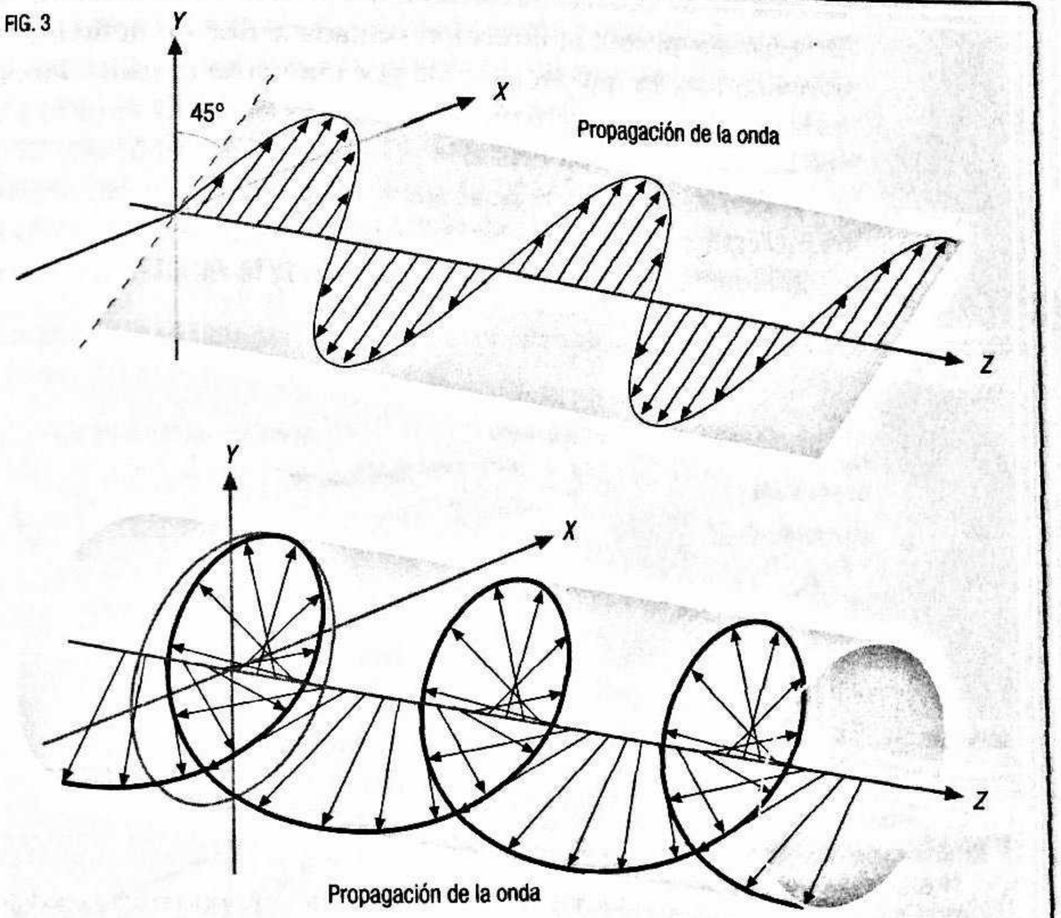
FIG. 2



Arriba, representación de una onda electromagnética plana linealmente polarizada. Los vectores campo eléctrico, $\vec{E}$, y campo magnético, $\vec{B}$, representados por flechas, oscilan manteniéndose siempre en sendos planos perpendiculares entre sí y a la dirección de propagación. En la figura, el plano de polarización se corresponde con el plano *OYZ*, mientras que la propagación se realiza según el sentido positivo del eje coordenado *Z*. Abajo se muestran los símbolos usuales para representar: a) luz despolarizada, b) luz polarizada verticalmente, c) luz polarizada en diagonal según un ángulo de 45°.

En general, son posibles también otros tipos de polarización, además de la lineal, como las polarizaciones circular y elíptica, en las que la punta de la flecha con que podemos representar la magnitud vectorial campo eléctrico avanza en el espacio describiendo bien un círculo, bien una elipse, como se ilustra para el caso circular en la figura 3, abajo. La luz natural, en la que no se

FIG. 3

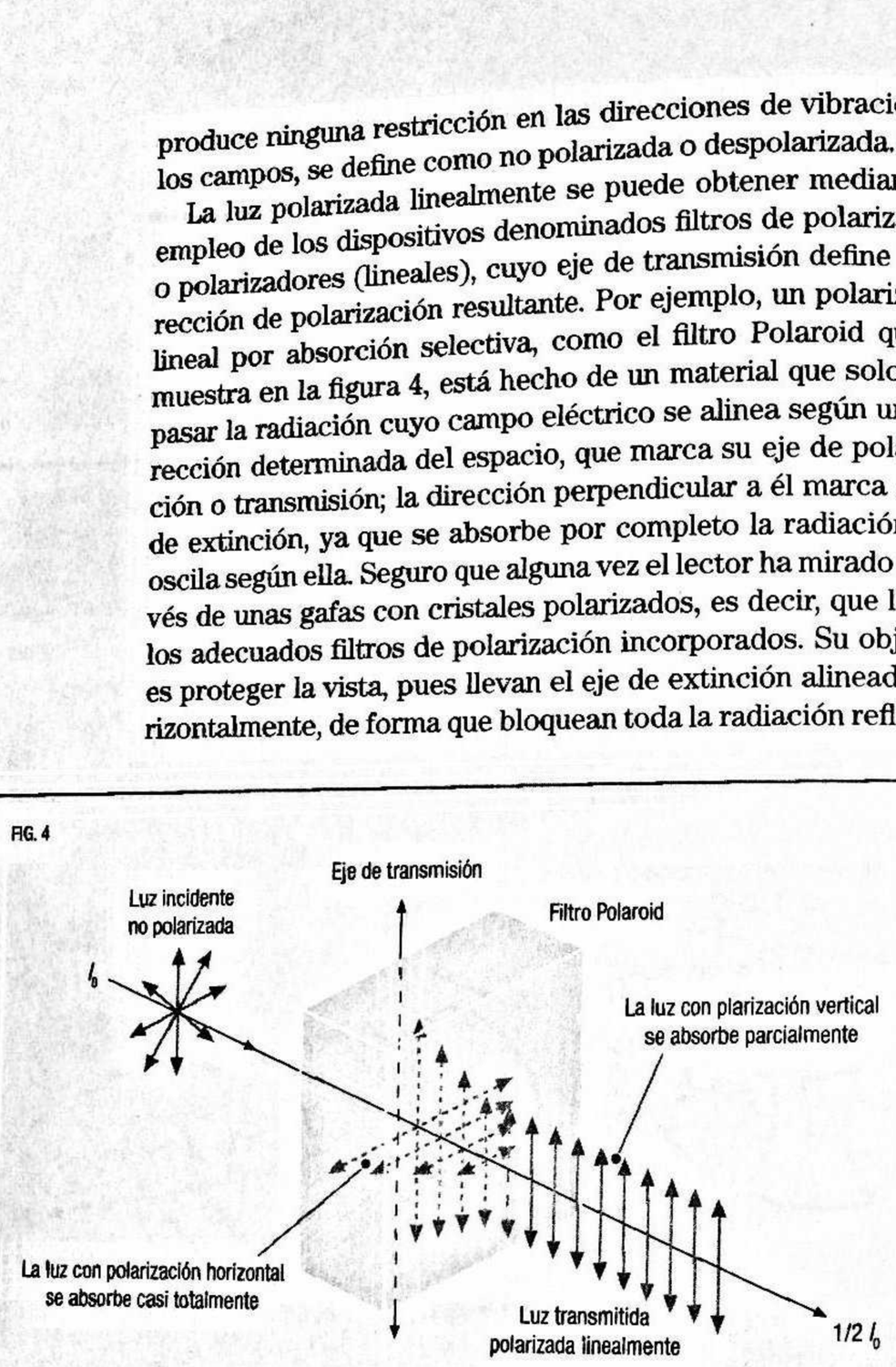


Arriba, luz polarizada diagonalmente con un ángulo de 45°. Abajo, luz polarizada circularmente: conforme la onda electromagnética avanza propagándose, la flecha que simboliza el valor del campo eléctrico en cada instante gira describiendo con su punta un círculo en el espacio.

produce ninguna restricción en las direcciones de vibración de los campos, se define como no polarizada o despolarizada.

La luz polarizada linealmente se puede obtener mediante el empleo de los dispositivos denominados filtros de polarización o polarizadores (lineales), cuyo eje de transmisión define la dirección de polarización resultante. Por ejemplo, un polarizador lineal por absorción selectiva, como el filtro Polaroid que se muestra en la figura 4, está hecho de un material que solo deja pasar la radiación cuyo campo eléctrico se alinea según una dirección determinada del espacio, que marca su eje de polarización o transmisión; la dirección perpendicular a él marca el eje de extinción, ya que se absorbe por completo la radiación que oscila según ella. Seguro que alguna vez el lector ha mirado a través de unas gafas con cristales polarizados, es decir, que llevan los adecuados filtros de polarización incorporados. Su objetivo es proteger la vista, pues llevan el eje de extinción alineado horizontalmente, de forma que bloquean toda la radiación reflejada

FIG. 4

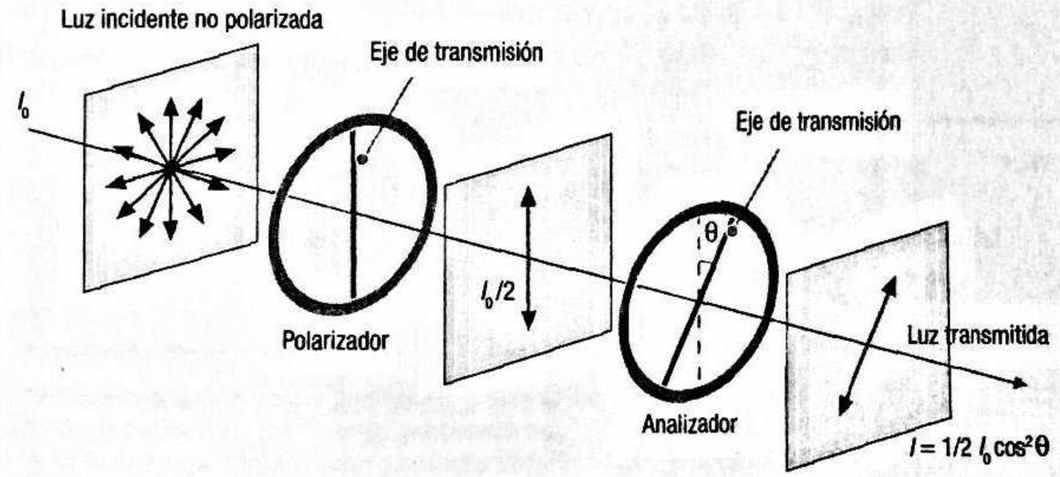


Acción de un filtro polarizador común, que convierte luz natural en luz polarizada linealmente según su eje de transmisión, con una pérdida usual del 50 % de la intensidad incidente, I_0.

en las superficies horizontales a nuestro alrededor, que en su mayor parte suele resultar con polarización horizontal, sobre todo en el caso de grandes superficies brillantes, como el mar o un suelo nevado.

El esquema de la figura 5 presenta lo que sucede cuando luz despolarizada atraviesa sucesivamente dos polarizadores lineales, el primero con su eje de transmisión vertical y el segundo formando un ángulo θ con dicha vertical. La luz saldrá del primer polarizador con polarización lineal vertical, y con su intensidad reducida a la mitad, ya que, como en una luz no polarizada la vibración se produce aleatoriamente según todas las direcciones del espacio, la energía o intensidad total se repartirá por igual entre todas esas direcciones y, en promedio, puede considerarse como dividida al 50% entre dos cualesquiera direcciones de vibración perpendiculares entre sí, una de ellas paralela al eje de transmisión. Esta luz, que sale del primer filtro ya polarizada verticalmente, entra a continuación al segundo polarizador

FIG. 5

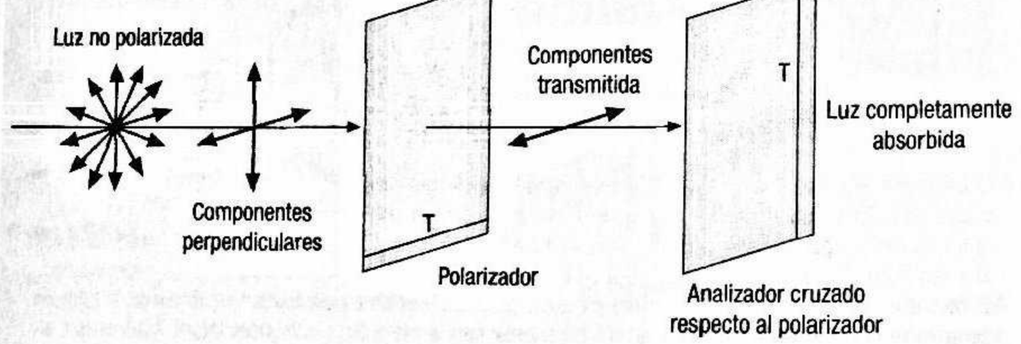


Acción sucesiva de dos polarizadores lineales sobre luz inicialmente no polarizada: tras atravesar el primero, orientado verticalmente, se transmite luz así polarizada, con la mitad de la intensidad inicial. Al atravesar el segundo polarizador, o analizador, cuyo eje está orientado formando un ángulo θ con la vertical, se transmite finalmente luz polarizada según dicho ángulo, con una intensidad que es una fracción $\cos^2\theta$ de la que incidió sobre él, un resultado conocido como ley de Malus.

(usualmente denominado analizador en estos montajes), que transmite a su vez luz polarizada según la dirección de su eje de transmisión (ángulo θ con la vertical), con una reducción de la intensidad adicional dada por el factor $\cos^2 \theta$, resultado que constituye la ley de Malus. Esta reducción de intensidad se produce debido a que la energía que transporta una onda electromagnética es proporcional al cuadrado del módulo de su vector campo eléctrico, el cual, tras pasar el analizador, se corresponde con la componente proyectada del vector $\vec{E}$ incidente sobre el eje de transmisión, es decir, $\vec{E} \cdot \cos \theta$. Por tanto, y puesto que el coseno de un ángulo recto, cos 90°, es nulo, si un haz de luz natural atraviesa dos polarizadores lineales consecutivos cruzados, es decir, con sus respectivos ejes perpendiculares entre sí, la intensidad se anulará y no se transmitirá luz alguna (figura 6).

Otra forma de obtener luz polarizada linealmente es hacer uso de los cristales birrefringentes, como la calcita o espato de Islandia, que tienen la propiedad de desdoblar la luz incidente, en general, en dos rayos linealmente polarizados de manera perpendicular entre sí. Existe una dirección particular en un material birrefringente en que ambos rayos se propagan con la misma velocidad, la cual define el eje óptico del cristal; si la incidencia es según esa dirección, no se observa desdoblamiento. La calcita

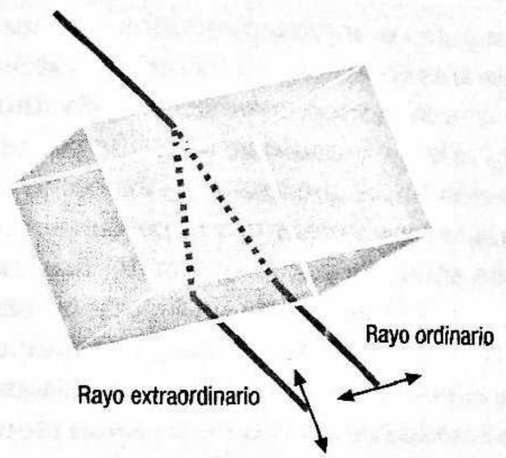
FIG. 6



Acción de dos polarizadores cruzados, es decir, con sus ejes de transmisión (indicados por las líneas T sobre cada polarizador) alineados de forma perpendicular entre sí: se anula cualquier transmisión de luz.

posee una birrefringencia acusada, fácil de constatar al advertir que a su través se forman dos imágenes distintas de cualquier punto situado detrás. La acción de este tipo de cristales se ilustra en la figura 7; para que se dé este efecto, el eje óptico del cristal no debe estar contenido en la cara tallada del cristal sobre

FIG. 7



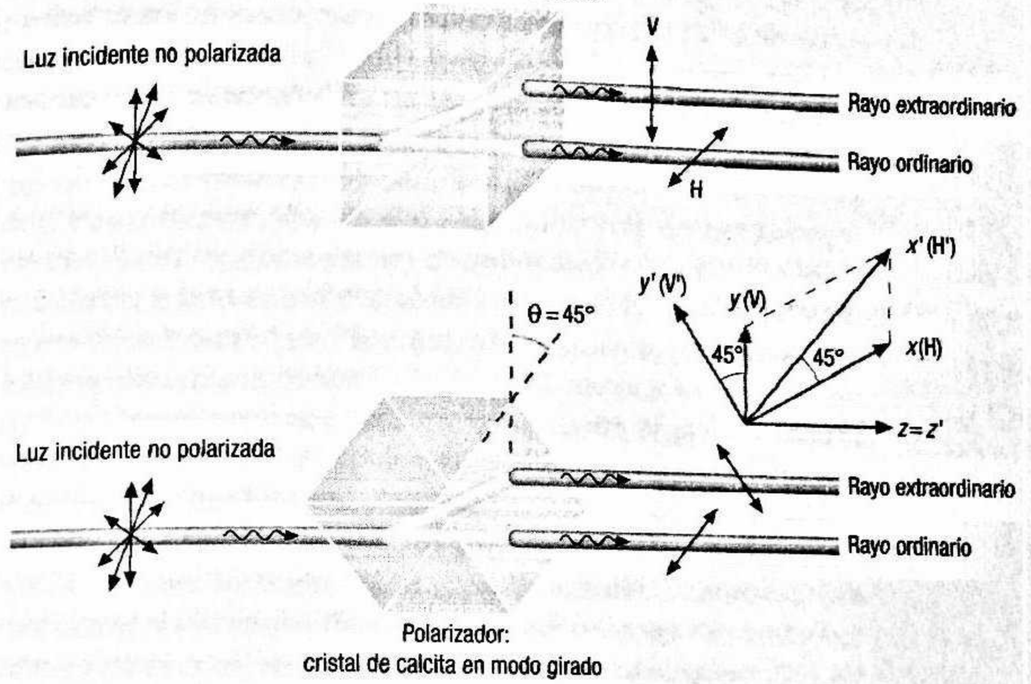
El esquema de arriba ilustra el desdoblamiento de la luz despolarizada al atravesar un cristal de calcita. Cuando la dirección de incidencia no se corresponde con el eje óptico, la luz se descompone en dos haces, polarizados siempre de forma perpendicular entre sí y según sendas direcciones determinadas por la dirección del eje óptico del cristal. El rayo que apenas se desvía es el denominado «ordinario», y es transmitido con polarización perpendicular al plano del cristal que contiene al eje óptico y a la dirección de incidencia. El rayo muy desviado se denomina «extraordinario» y resulta con polarización perpendicular a la del rayo ordinario y paralela a la dirección del eje óptico del cristal. Abajo, imagen doble de un texto a través de un cristal de calcita.

la que se produce la incidencia, ni ser perpendicular a ella. Una ventaja adicional frecuente en ellos es que la absorción de la radiación que los atraviesa suele ser mínima.

Los fotones y su polarización en mecánica cuántica

En términos cuánticos, incorporando los fotones, cuando luz no polarizada sale tras atravesar un cristal de calcita, orientado en el espacio de una manera conveniente, cada uno de los fotones que componen el haz ordinario se describe por un estado cuántico de polarización lineal que asumiremos como «horizontal», estado que vamos a representar por el símbolo →. Análogamente, los fotones que salen formando parte del haz extraordinario se describen por una función de onda o estado cuántico de polarización lineal que convendremos en fijar como «vertical», y que simbolizaremos como ↑. La descripción teórica que incorpora estos tipos de estados cuánticos de un fotón reemplaza con ellos las menciones de un campo eléctrico oscilando en una dirección, horizontal o vertical, que se corresponden con la descripción clásica. Por supuesto, «horizontal» y «vertical» se asimilan a cualesquiera dos direcciones del espacio mutuamente perpendiculares, H y V, y que son seleccionadas por la orientación en el espacio de la calcita empleada (por la dirección en la que se haya alineado su eje óptico, en definitiva), según se muestra en la figura 8. También podríamos elegir, por ejemplo, las dos direcciones del espacio que forman 45° y 135°, respectivamente, con la tomada antes como horizontal, H, cuyos correspondientes estados cuánticos de polarización fotónica simbolizaremos como ↗ y ↘, denominándolos estados de polarización diagonal (respecto al anterior sistema de ejes horizontal-vertical). Para generar fotones en estos estados diagonales, bastará con orientar la calcita de forma girada respecto a la anterior, o sea, haciendo que su eje óptico esté girado en el espacio 45° respecto a la anterior posición recta (modo R); denominaremos a esta segunda orientación de la calcita modo girado o diagonal (modo D), representado en el esquema inferior de la figura 8.

FIG. 8



Arriba, un medidor o determinador de polarización fotónica horizontal-vertical: se trata de un cristal de calcita orientado en modo recto, es decir, con la orientación de su eje óptico de modo que un fotón al atravesarlo salga bien con polarización según la dirección que hemos convenido en fijar como «horizontal», H (cuando sale como rayo ordinario, sin desviación y estado de polarización lineal →) o «vertical», V (rayo extraordinario, muy desviado y polarizado según una dirección perpendicular a la anterior, estado ↑). Abajo, el mismo cristal en modo girado 45°, o modo diagonal: ahora los fotones que salen en el rayo ordinario y extraordinario, respectivamente, según las direcciones H' y V', corresponden a fotones en los estados fundamentales de polarización lineal ↗ y ↘.

Introducido un par cualquiera de estados de polarización fotónicos fundamentales, esto es, que representen sendas polarizaciones lineales según dos direcciones mutuamente perpendiculares en el espacio, como el par (→, ↑) o (↗, ↘), o cualquier otra elección similar, el estado cuántico más general de polarización que puede ocupar un fotón individual en cada instante es la superposición de los estados componentes de ese par, es decir, la suma:

$$\psi = a \cdot \rightarrow + b \cdot \uparrow$$
$$= c \cdot \nearrow + d \cdot \searrow$$

En definitiva, podríamos optar por superponer los estados del par fundamental horizontal-vertical, o diagonal, o cualquier otro. En este estado superpuesto, salvo que uno de los dos números coeficientes a o b (que pueden ser complejos) sea cero, la polarización está indeterminada; los números reales positivos $|a|^2$ y $|b|^2$ representan las probabilidades teóricas de que, al hacer que el fotón atraviese un analizador de polarización, el resultado de la polarización medido sobre el fotón sea horizontal o vertical, respectivamente (con interpretación análoga para c y d, ahora para las dos polarizaciones diagonales). Debido a esta interpretación probabilística, la suma de estos dos números debe ser 1, una condición que se dice que «normaliza» la distribución de probabilidad ψ. Por supuesto, en coherencia con la indivisibilidad de un cuanto de luz, cada medida producirá, sobre cada fotón, uno de los dos resultados posibles, y solo uno.

Veamos un ejemplo. La luz natural, despolarizada por completo, está compuesta de fotones a los que se les asocia el estado cuántico de superposición:

$$\psi = \left(1/\sqrt{2}\right) \cdot \rightarrow + \left(1/\sqrt{2}\right) \cdot \uparrow$$

cuyos coeficientes proporcionan igual probabilidad del 50 % ($\left|1/\sqrt{2}\right|^2 = 0{,}50$) para los dos resultados posibles de toda medida de la polarización de cada fotón individual, horizontal o vertical. En cambio, para otros tipos de luz, en los que el fotón esté inicialmente en un estado polarizado, por ejemplo, en el estado polarizado horizontal (estado ψ para el que $a = 1$ y $b = 0$), entonces la probabilidad de que al medir su polarización se obtenga un resultado horizontal será 1, o sea, el fotón siempre atravesará un polarizador lineal orientado horizontalmente. Por supuesto, nunca lo hará en este caso si la orientación del analizador se dispone en vertical.

A partir de los estados fundamentales de polarización que hacen posible la descripción cuántica elemental de la radiación, estamos en condiciones de interpretar cuánticamente lo que sucede en la figura 5, donde incide radiación no polarizada. Frente al primer polarizador, orientado verticalmente, se tiene un 50 % de probabilidad (ya que $\left|1/\sqrt{2}\right|^2 = 0{,}50$) para cada fotón de atravesarlo. Suponiendo que uno de ellos lo consiga —solo se transmitirán la mitad de todos los fotones incidentes—, después de la transmisión pasará a estar descrito por el estado vertical. A continuación, cada fotón sobreviviente al primer analizador tiene una probabilidad $\cos^2\theta$ de transmisión en el segundo analizador. Es decir, la ley de Malus se deriva también en el formalismo cuántico, pero pasa a ser interpretada en términos probabilísticos. La descripción, por lo tanto, incorpora el puro azar en el siguiente sentido: cuando muchos fotones individuales —no polarizados— inciden sobre el dispositivo, no es posible prever lo que pasará con cada uno de ellos. La teoría solo predice que, cuando el número total de fotones que han incidido sea suficiente, se habrá transmitido tras los dos polarizadores la fracción $\cos^2\theta$ de la mitad del número total de ellos incidentes que marca la ley de Malus (suponiendo absorciones ideales en los filtros).

> El único objetivo de la física teórica es calcular resultados que se puedan comparar con la experiencia [...]. Es totalmente innecesario que deba darse una descripción satisfactoria del curso completo de los fenómenos.
>
> **Paul Dirac**

Los cristales birrefringentes, como la calcita, nos proporcionan un medio de medir la polarización lineal de un fotón sin riesgo elevado de perderlo por absorción en el dispositivo, ya que, con la adecuada preparación, no absorben casi ningún fotón incidente. ¿Podemos prever lo que pasará a la salida del cristal con cada fotón de un haz incidente? O, planteado de forma equivalente, si suponemos que la luz que incide sobre la calcita lo hace fotón a fotón, ¿qué sucederá con cada fotón individual? ¿Sufrirá gran desviación o no? Es decir, ¿hará transmisión extraordinaria o normal? Porque cada fotón individual es indivisible, de modo que no puede repartirse entre los dos tipos de transmisiones. En el formalismo cuántico, como ya sabemos, la respuesta es —en general— probabilística: la teoría solo establece la probabilidad

de cada fotón individual de acabar con polarización lineal de un determinado tipo, de entre dos modos perpendiculares, y no es posible saber de antemano qué suerte experimentará cada fotón concreto.

Al salir de la calcita un fotón transmitido como rayo ordinario, su descripción cuántica pasa a ser un estado polarizado horizontalmente. Se ha producido el colapso de la función de onda superpuesta anterior, la que proporcionaba su descripción cuántica antes de su interacción con la calcita como una superposición de los dos estados de polarización; para un fotón que abandona la calcita como rayo extraordinario, el colapso se ha producido hacia el estado de polarización vertical. El cristal de calcita, por tanto, nos ilustra cómo actúa un aparato de medida en mecánica cuántica: provoca la determinación de la variable que mide, en este caso la polarización lineal. La medida deshace la superposición cuántica, colapsando la función de onda hacia un estado en que la propiedad medida podría decirse que está bien determinada (en el sentido de que hay un 100% de probabilidad de encontrar de nuevo ese valor obtenido la primera vez, si se repite a continuación sobre el sistema la misma medida).

¿Y qué pasará cuando el fotón incidente sobre un cristal de calcita venga ya polarizado linealmente? Es decir, si ese fotón ha atravesado antes un filtro de polarización que ha determinado su estado hacia uno fundamental, ¿por cuál de los dos canales de salida va a transmitirse? La respuesta está clara: depende de la orientación relativa entre la polarización que trae y la del eje óptico de la calcita. En particular, cuando lo que incide sobre el cristal de calcita orientado en modo recto, o modo horizontal-vertical, es un fotón polarizado horizontalmente, estado → ($a=1$ y $b=0$), entonces siempre —100% de probabilidad— saldrá por el canal ordinario (apenas se desvía y no se altera su polarización); si incide un fotón polarizado verticalmente, estado ↑ ($a=0$ y $b=1$), entonces se tiene un 100% de probabilidad —certeza— de que saldrá por el canal extraordinario (desviándose de nuevo, pero conservando la polarización vertical). Pero si lo que incide es un fotón polarizado diagonalmente (en uno de los dos

estados ↗ o ↘), entonces sucederá lo mismo que para luz despolarizada: 50% de probabilidad para cada fotón de emerger por el canal ordinario (polarización final determinada horizontal) o por el extraordinario (polarización determinada vertical).

La calcita en modo recto, pues, nos proporciona un método eficaz para lograr separar un haz de fotones en dos grupos caracterizados por uno de los dos valores, horizontal o vertical, de una variable física dicotómica, la polarización lineal. Puesto que la unidad de medida de la cantidad de información es el *bit*, equivalente a la elección entre dos posibilidades igualmente probables, 0 y 1, la calcita nos proporciona un mecanismo de implementación física para una serie de bits cuánticos fundamentales, que tomamos como 0^Q cuando la polarización es horizontal, y 1^Q para la vertical. Por supuesto, es solo una convención: de forma por completo equivalente podríamos haber hecho la elección al revés. Estos dos *qubits* fundamentales se suelen denominar «básicos», y serán usados con eficacia para codificar información, según veremos en los capítulos siguientes. El estado general de superposición cuántica de los dos qubits fundamentales:

$$\Psi = a \cdot 0^Q + b \cdot 1^Q,$$

constituye el qubit general, sin correlato clásico. Como vemos, podremos implementarlo sobre fotones, asimilándolo con un estado de polarización general $\Psi = a \cdot \rightarrow + b \cdot \uparrow$. Las direcciones mutuamente perpendiculares (ortogonales) que selecciona la calcita se pueden cambiar sin más que girar el cristal de calcita, en torno a la dirección de incidencia, un ángulo dado, puesto que así cambiará la dirección de su eje óptico. Por ejemplo, si este ángulo se toma como de 45° respecto a la orientación recta, con la calcita en modo diagonal (véase la imagen inferior de la figura 8), el qubit general tomará la expresión $\Psi = c \cdot \nearrow + d \cdot \searrow$.

En resumen, «medir» la polarización de un fotón no se entiende en física cuántica igual que en física clásica, es decir, se entiende de una manera que no es la usual en nuestro lenguaje natural. En cuántica, la medida de muchas propiedades, como

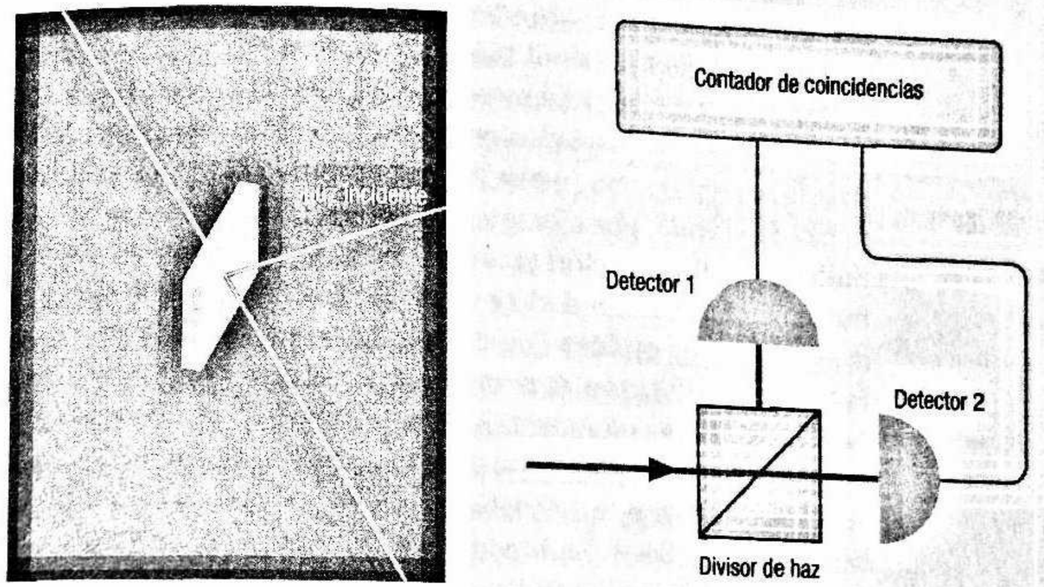
la polarización fotónica, no se concibe como una intervención sobre un sistema que nos informa sobre cuál era antes —y cuál es tras la medida— el valor de la propiedad sobre ese sistema, sino que es una interacción que provoca que la propiedad medida se determine en un valor, estando antes, en general, indeterminada. Las propiedades para las que esto sucede son aquellas respecto a las cuales el sistema cuántico puede ocupar estados del tipo superpuesto, y se definen como propiedades «contextuales». La energía, la polarización, la posición, el momento y el espín (que veremos a continuación) son algunos ejemplos de propiedades contextuales.

En este libro nos limitaremos a una descripción de los fotones por estados cuánticos asociados a la propiedad física polarización, sin entrar en más consideraciones e intentando no imaginar al fotón como una partícula —aunque así lo llamaremos—, ni tampoco como una «onda-partícula». La descripción del fotón escapa a las analogías clásicas.

Cómo comprobar si una luz es monofotónica

Muchos de los experimentos que vamos a mencionar se realizan, idealmente, utilizando luz monofotónica, es decir, radiación compuesta por pulsos que contienen un solo fotón, una situación que se describe a veces diciendo que la incidencia de la radiación es con «fotones uno a uno». Disponer en la práctica de una fuente de luz monofotónica no es fácil, porque, para conseguir auténtica radiación monofotónica, no basta en rigor con atenuar mucho la intensidad de la radiación incidente. ¿Cómo puede entonces garantizarse que la luz empleada es auténticamente monofotónica? Por ejemplo, mediante un dispositivo como el mostrado a la derecha en la figura 9, que certificará el carácter monofotónico de la radiación incidente cuando los dos detectores de radiación presentes nunca detecten radiación al mismo tiempo. El diseño integra un divisor de haz o espejo semirreflector, un dispositivo en el que un haz de luz incidente es en parte reflejado y en parte transmitido —usualmente al 50 %—,

FIG. 9



A la izquierda, representación de la acción de un divisor de haz: cada fotón incidente tiene cierta probabilidad de ser reflejado o transmitido (las probabilidades suman el 100 %). En ausencia de observación, la función de onda describe la situación como una superposición de las dos posibilidades, pero, en cada medida o detección, solo se realiza una de las dos. A la derecha, un montaje experimental que nos permite decidir si una radiación incidente es monofotónica o no: si lo es, el contador de coincidencias entre dos detectores colocados en ambos lados del divisor de haz nunca registrará una coincidencia temporal de señal o registro de radiación simultáneo en ambos detectores.

según se muestra ampliado a la izquierda en la misma figura. En el caso de que se hagan incidir sobre el divisor de haz pulsos de luz monofotónica, esto es, fotones de uno en uno, no hay manera de conocer de antemano cuál de las dos posibilidades, reflexión o transmisión, va a ser observada para cada fotón individual. Es decir, en ausencia de observación la función de onda que se asocia al sistema es una superposición cuántica de dos posibilidades, un sumando describe el fotón transmitiéndose y el otro, el fotón reflejándose. Eso sí, para cada fotón individual solo se realizará la observación de una de las dos posibilidades, de manera que nunca los dos detectores señalarán a la vez la detección de un fotón.

EL ESPÍN, UNA MAGNITUD PURAMENTE CUÁNTICA

El momento angular —también llamado momento cinético— es una importante magnitud física, de carácter vectorial. Un ejemplo lo proporciona el momento angular orbital de una partícula que realiza un movimiento en órbita circular alrededor de otro, bajo la acción de una fuerza central (dirigida hacia un punto fijo, como es el caso, por ejemplo, de la Luna alrededor de la Tierra, bajo la mutua atracción gravitatoria). El módulo del vector momento angular viene dado por el producto $m \cdot v \cdot r$, es decir, de la masa por la rapidez (módulo del vector velocidad) y por el radio de la órbita; su dirección es perpendicular al plano de la órbita. En física cuántica, tanto las partículas cargadas como las neutras, las materiales o los fotones, poseen espín, un momento angular intrínseco, no asociado a ningún tipo de movimiento y sin análogo clásico. La incorporación a la teoría de esta nueva magnitud vectorial es indispensable para explicar un gran número de observaciones experimentales, y asociado a él se introduce el denominado *número cuántico de espín*, s; las partículas para las que s es nulo o entero ($s = 0, 1, 2, 3...$) se llaman *bosones*, mientras que las partículas para las que s toma valores semiimpares ($s = 1/2, 3/2, 5/2...$) se denominan *fermiones*.

En relación con el momento angular, numerosos experimentos han confirmado el fenómeno de su cuantización, que se manifiesta de dos maneras. En primer lugar, por el hecho de que el módulo de un momento angular en mecánica cuántica solo puede tomar determinados valores, que en particular para el caso del espín vienen dados en términos del número cuántico s por la expresión:

$$\left|\vec{S}\right| = \hbar\sqrt{s(s+1)},$$

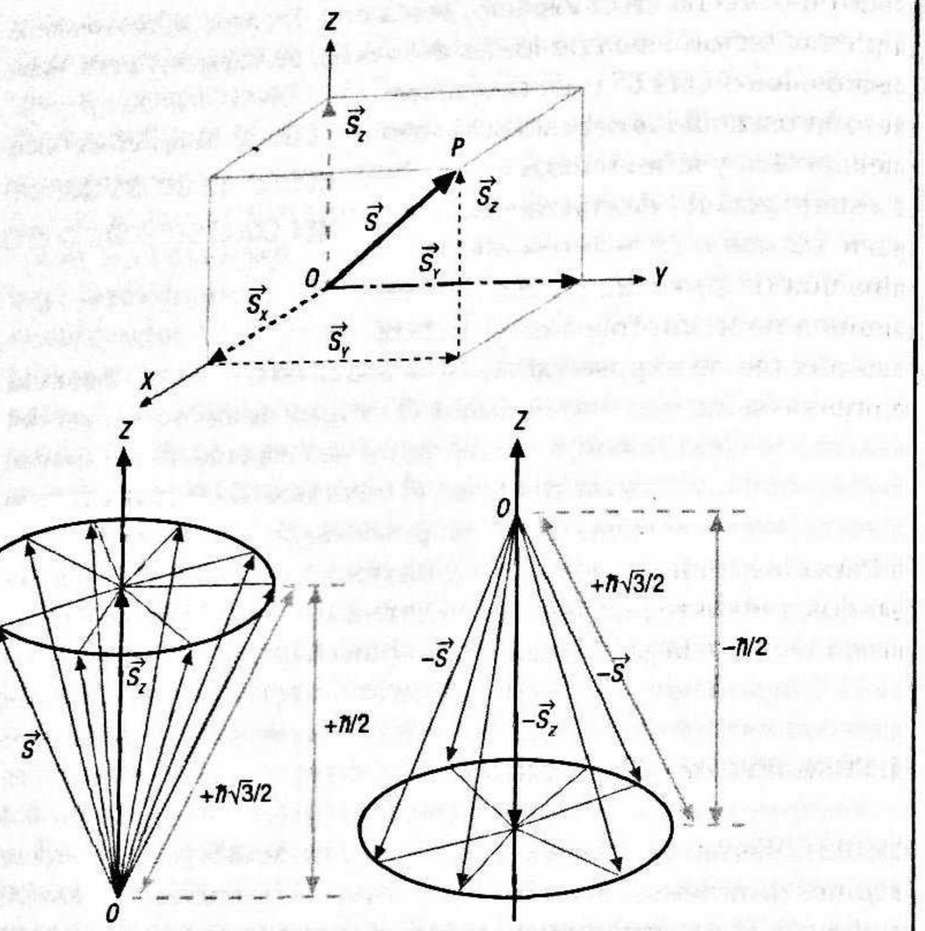
donde $\hbar$ es la constante de Dirac o constante de Planck reducida (esto es, dividida por el factor numérico 2π), cuyo valor es $1{,}0545716 \cdot 10^{-34}$ J·s. En segundo lugar, por la denominada «cuantización espacial», un fenómeno también comprobado experimentalmente de forma exhaustiva. Para entenderlo, primero

necesitamos recordar que, para especificar un vector determinado, una flecha en el espacio, basta con dar tres números reales, denominados componentes del vector en un sistema de ejes coordenados *OXYZ*. Esos tres números representan los módulos de otros tres vectores, sobre sendos ejes, cuya suma es igual al vector en cuestión. La parte superior de la figura 10 ilustra esta descomposición en tres componentes vectoriales ($\vec{S}_X$, $\vec{S}_Y$, $\vec{S}_Z$) para el caso del vector representativo de un espín, de módulo S, indicado como la flecha que une el punto O, origen de coordenadas del sistema de ejes tomado, con un punto P del espacio. Introducidas así las componentes de un vector, el fenómeno de la cuantización espacial consiste en que solo son posibles, para una componente dada, por ejemplo la tercera, $\vec{S}_Z$, un número limitado de valores. En física clásica, por el contrario, no surge esta limitación, y el rango de valores permitidos para el módulo y la orientación de cada componente del vector momento angular no es discreto, sino continuo, de modo que entre dos posibles valores, todos los intermedios son también posibles. Es decir, no hay cuantización.

> Todo lo que llamamos real está hecho de cosas que no pueden ser consideradas como reales.
>
> **Niels Bohr**

Veámoslo con la imagen inferior de la figura 10, que muestra las posibles orientaciones espaciales permitidas para el vector espín $\vec{S}$ y su vector tercera componente, $\vec{S}_Z$, correspondientes a una partícula con número cuántico de espín $s = 1/2$ (por ejemplo, un electrón). La tercera componente de su momento angular intrínseco solo tiene dos posibilidades, que se suelen denominar espín «hacia arriba», símbolo ↑, y espín «hacia abajo», ↓, ambas de módulo $\hbar/2$. Si imaginamos un haz de electrones que se propagan en una región del espacio en la que no hay ningún dispositivo experimental preparado para medir espines, ¿cuál es entonces la descripción mecanocuántica para el estado de espín de cada electrón? Pues una función de onda que encierra matemáticamente el hecho de que, antes de haber sido sometido a una medida de la orientación espacial de su espín, el electrón no tiene determinada dicha orientación de su espín. Es decir, este se halla en un estado de superposición de todas las

FIG. 10



En la imagen superior, un vector $\vec{S}$ y sus respectivas componentes vectoriales $\vec{S}_x$, $\vec{S}_y$ y $\vec{S}_z$ sobre los tres ejes coordenados *X*, *Y*, *Z*. Abajo: para un vector espín $\vec{S}$, correspondiente a una partícula con número cuántico de espín $s = 1/2$, de módulo $S = \hbar\sqrt{1/2(1/2+1)} = \hbar\sqrt{3}/2$, una vez marcada una dirección posible en el espacio como eje *OZ*, solo son posibles ciertas orientaciones de $\vec{S}$ respecto a ella: las que se corresponden con un vector componente $\vec{S}_z$ de módulo $\hbar/2$, coincidentes con las generatrices de los dos conos representados (solo algunas de ellas se han dibujado, como flechas sobre cada superficie cónica y con origen en *O*). Aparecen, pues, dos posibilidades para el vector $\vec{S}_z$: orientarse según el sentido positivo de eje *OZ* (resultado de la tercera componente de espín «hacia arriba», usualmente representado como ↑, imagen inferior izquierda) o, sobre la misma dirección, tomar el sentido opuesto (tercera componente de espín «hacia abajo», ↓, imagen inferior derecha).

posibles orientaciones compatibles con la cuantización espacial del mismo, sin que pueda suponerse que posee de forma determinada ninguna de ellas.

El espín de un fermión con número cuántico $s = 1/2$, como un electrón o algunos átomos, nos proporciona otro recurso para la implementación física de los qubits cuánticos fundamentales o básicos, los qubits 0^Q y 1^Q. Basta con hacer corresponder al primero la partícula en el estado de tercera componente de espín hacia arriba, y al segundo, en el estado hacia abajo (o al revés). El estado general de superposición cuántica de una partícula de espín 1/2 que no ha sido sometida a un experimento de determinación de su espín, por su parte, se corresponde en la teoría cuántica de la información con el qubit general, de forma análoga a como se expuso para el caso fotónico; en este caso, su expresión será:

$$\Psi = a \cdot \uparrow + b \cdot \downarrow = a \cdot 0^Q + b \cdot 1^Q.$$

Para conseguir situar las partículas individuales en este tipo de estados, puede recurrirse, por ejemplo, a confinarlas en «trampas», mediante la aplicación de campos electromagnéticos.

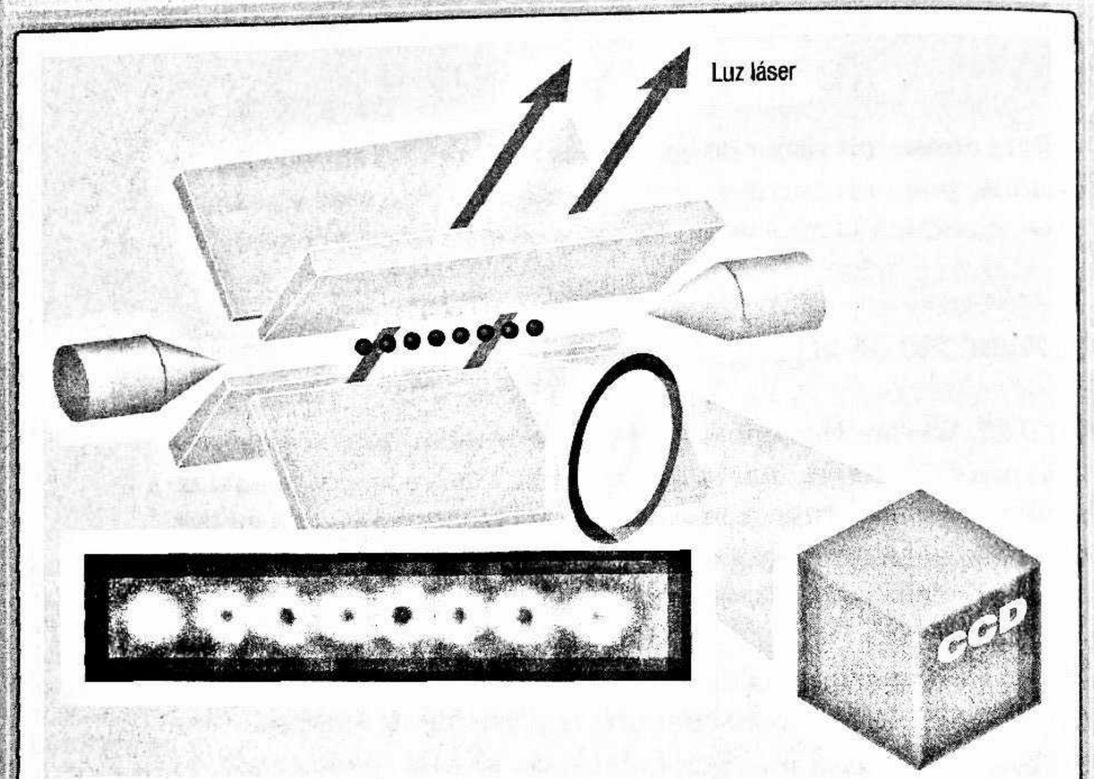
EL PRINCIPIO DE INDETERMINACIÓN

En 1927, Werner Heisenberg publicó la primera versión de las relaciones de indeterminación; según esta, cuanta mayor precisión se alcanza al determinar la posición de una partícula, con menor precisión se puede conocer su momento lineal (el producto de la masa por la velocidad), y viceversa.

¿Cuál es el principal significado riguroso moderno del principio de indeterminación? Para comprenderlo, es imprescindible considerar que la teoría cuántica, a partir de la interpretación probabilística para la función de onda, es una teoría estadística. Como tal, en ella juega un papel importante el concepto de *valor medio* de una propiedad, que vamos a explicar a continuación. Si queremos determinar experimentalmente, por ejemplo, la posición de una partícula, necesitaremos disponer de muchos sistemas iguales, compuestos todos por el mismo tipo de partícula, preparada además en las mismas condiciones, de forma

TRAMPAS PARA IONES

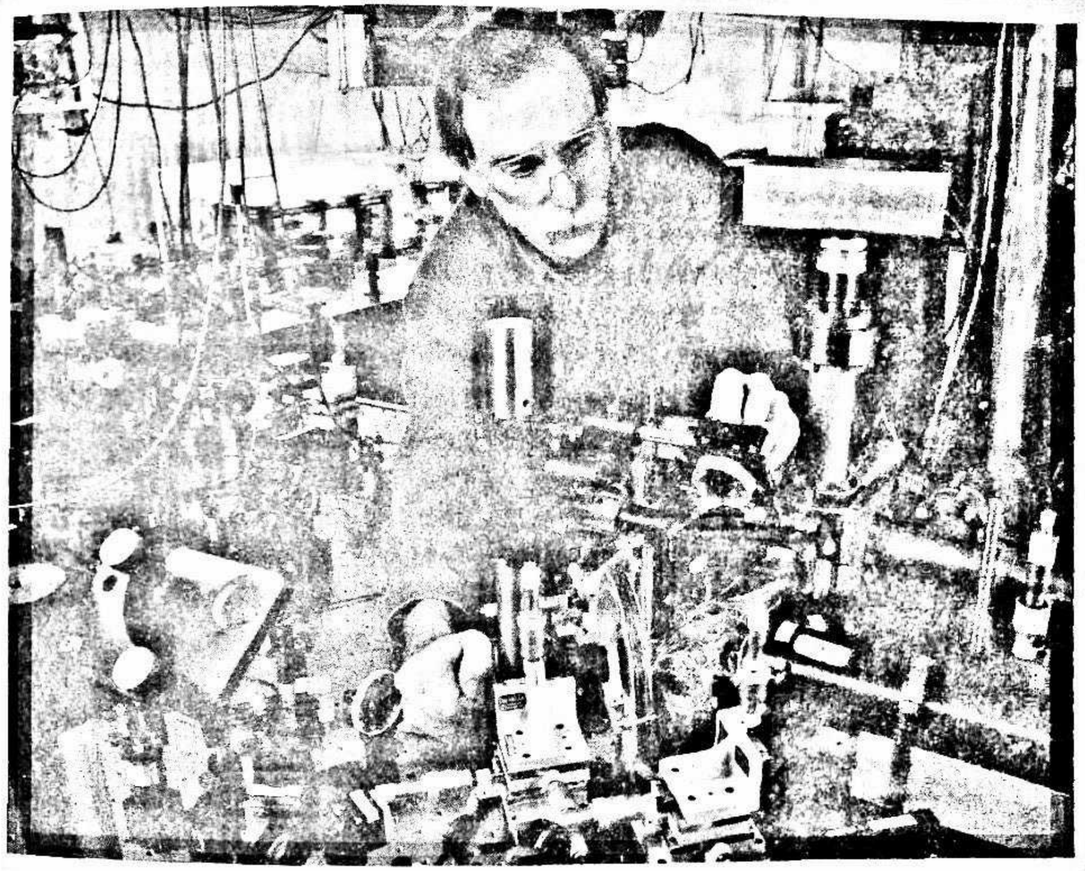
El procesado cuántico de la información necesita desarrollar métodos que permitan manipular los estados de los entes cuánticos individuales. En este siglo, se ha empezado a lograrlo no solo con fotones, sino también con partículas materiales. Para ello se pueden usar trampas de iones, dispositivos en los que se consigue confinar iones individuales, aislándolos del exterior. El procedimiento consiste en generar unos campos variables, mediante los adecuados electrodos, de forma que los iones están sometidos a potenciales oscilantes con valores según dos direcciones perpendiculares del espacio, ejes *OX* y *OY*, mucho mayores que en la tercera, el eje *OZ*, lo que provoca el alineamiento de los iones según esta última dirección. Una vez así situados, se actúa sobre ellos con láseres, consiguiendo controlar su temperatura y, al enfriarlos, se logra «pararlos», quedando preparados en el estado más bajo en energía posible para el sistema conjunto, con unas distancias entre los iones de unos micrómetros.



Esquema de la trampa de iones de Blatt y Wineland. Mediante pulsos de luz láser se manipula el estado cuántico de ocho iones calcio (alineados dentro de la trampa). Para detectarlo, se mide la fluorescencia de los iones en una cámara CCD *(Charge-Coupled Device)*. La presencia o no de fluorescencia, relacionada con la transición desde un tercer estado cuántico auxiliar, señala el estado fundamental particular de cada qubit. En la imagen, el espacio entre los dos iones centrales es de unos 8 μm.

Fabricando qubits con iones de calcio

Son ya bastantes los laboratorios que están desarrollando trampas de iones, con diversos prototipos. En 2008, Rainer Blatt y David Wineland, del NIST (*National Institute of Standards and Technology*, Instituto Nacional de Normas y Tecnología de los Estados Unidos), construyeron una trampa para iones de calcio cuyo esquema se presenta en la figura de la página anterior, con ocho iones separados entre sí por una distancia de aproximadamente 8 μm. Usando una trampa similar, en 2014 Thomas Harty y sus colaboradores implementaron varios qubits en la Universidad de Oxford, a partir de los estados de energía individuales de dos iones de calcio. El procedimiento consiste en tomar como qubits básicos 0^{o} y 1^{o} los respectivos estados de energía E_1 y E_2 de cada átomo individual, algo factible porque, al tenerlos confinados en la trampa, es posible manipularlos uno a uno, usualmente aplicándoles pulsos de luz láser. De esta forma, también lograron preparar estados entrelazados con ellos.



David Wineland, físico del NIST, ajusta el láser para manipular los iones contenidos en una trampa. El desarrollo de las trampas de iones es muy importante para las nuevas tecnologías cuánticas de procesamiento y distribución de información, como la computación cuántica.

que cada uno de los sistemas individuales de la colección tenga asociada la misma función de onda Ψ (venga descrito por ella). Medimos entonces, sobre cada sistema individual y con idéntico procedimiento, la posición de la partícula, y obtenemos así una colección de resultados, tantos como sistemas análogos hayamos dispuesto. La media de todos ellos, es decir, el valor que resulta al sumarlos todos y dividirlos por su número total, es lo que se conoce como valor medio de la propiedad (posición, en el ejemplo) sobre el sistema. Este valor medio es, pues, un concepto estadístico, que en general no tiene por qué coincidir con uno de los resultados, aunque puede hacerlo; tampoco tiene por qué coincidir con el valor más probable o frecuente.

En este marco matemático estándar, apareció una característica nueva que, en los inicios de la teoría, resultó desconcertante: la predicción teórica de que, cuando se llevaran a cabo las experiencias de medida de algunas parejas de propiedades de un sistema, por ejemplo, posición y momento de una partícula, el resultado no sería el mismo si primero se medía la posición y luego el momento, que si se hacía con el orden cambiado. La predicción resultó acertada, y se incorporó al formalismo definiendo que los pares de propiedades para las que esto sucedía eran *complementarias* o «incompatibles», mientras que aquellas para las que los resultados de su medida eran indiferentes al orden se establecieron como «compatibles».

La consideración de las propiedades complementarias conduce inexorablemente al principio de indeterminación, que no es, pues, postulado, sino teorema demostrable matemáticamente a partir de la existencia constatada de pares de propiedades incompatibles. Su enunciado incorpora la consideración de una cantidad $\Delta_\psi A$, denominada indeterminación fundamental cuántica de la propiedad A, sobre un estado Ψ dado, el análogo cuántico de la desviación estándar, el parámetro estadístico usual que mide cuánto se separan o dispersan los datos de una colección de valores respecto a su valor medio. Dicho de otra manera, Δ^2 se corresponde con la varianza o cuadrado de la desviación estándar estadística: la media de los cuadrados de las diferencias con la media de todas las medidas, bien entendido que «todas las

medidas» refiere, como antes, al conjunto de resultados obtenidos al medir una misma propiedad física sobre muchos sistemas análogos y preparados de la misma forma. Esta indeterminación así definida es siempre real y positiva o nula, y el principio fundamental de indeterminación —conocido también como principio de Heisenberg— establece que, sobre cualquier estado Ψ de un sistema, en la medida de dos propiedades complementarias el producto de las respectivas indeterminaciones no puede ser menor que cierto valor numérico no nulo (que es, usualmente, del orden de la constante de Planck). En términos de información, establece una cota para la cantidad de información que podemos extraer de los sistemas físicos. Por ejemplo, para una partícula material libre, nos muestra que es imposible concebir un experimento que permitiera determinar a la vez su posición y momento, con indeterminaciones respectivas que violaran el principio.

Por el principio de indeterminación, hay propiedades de un sistema que no van a poder ser medidas de forma simultánea con precisión ilimitada, por una restricción de orden fundamental, inviolable, y no solo por las típicas limitaciones operativas prácticas relacionadas con la pericia del experimentador y la calidad del aparato empleado (que también están presentes en la física cuántica, como en la clásica). Las relaciones de indeterminación no restringen la precisión con que un solo observable puede medirse, sino la precisión con que pueden medirse simultáneamente dos observables no compatibles, como la posición y el momento de una partícula material. La medida de una propiedad particular sobre un sistema físico se ve instantáneamente acompañada de una alteración de las distribuciones de probabilidad para los resultados de las medidas de las propiedades complementarias a la que se mide. Para reflejar esa alteración se postula un cambio de la función de onda que describe el sistema, cambio expresado en el proceso matemático denominado colapso o reducción de dicha función, y hace que la información máxima a que podemos acceder sobre un sistema esté limitada: no puede incluir especificación simultánea de observables complementarios entre sí, más allá de los límites que establece el principio de indeterminación.

La imposible duplicación cuántica

El teorema de no duplicación (o no clonado) cuántico fue formulado en 1982 por William Wootters, Wojciech Zurek y Dennis Dieks, y establece una consecuencia directa del principio de indeterminación: no es posible que exista un dispositivo que pueda duplicar exactamente cualquier estado cuántico arbitrario desconocido. Es fácil de argumentar a partir del principio de indeterminación: puesto que al medir una propiedad alteramos las distribuciones de probabilidad para los resultados de las medidas de las propiedades complementarias a ella, y puesto que no podemos medir simultáneamente observables complementarios con tanta precisión como queramos, es imposible acceder a toda la información requerida para duplicar el estado. O, visto de otra forma: si se pudiesen realizar esas copias perfectas, sería porque se habría podido extraer la máxima información requerida sobre el sistema, abriéndose entonces la posibilidad de medir magnitudes incompatibles más allá de los límites que impone el principio de indeterminación. En efecto, se podrían medir dos de ellas sin límite de precisión fundamental, haciéndolo de manera independiente en sendas réplicas o clones. Luego la consistencia de la teoría cuántica exige que no sea posible realizar dichas copias.

Esta imposibilidad de realizar el clonado de un sistema cuántico implica una de las grandes diferencias que nos vamos a encontrar en la teoría cuántica de la información respecto a la teoría clásica. Nos va a impedir, por ejemplo, acudir a la técnica de la redundancia, es decir, a almacenar la misma información en registros repetidos, con el fin de controlar los posibles errores en su transmisión.

EL DESCONCERTANTE ENTRELAZAMIENTO

El *entrelazamiento* es una propiedad que poseen algunos estados cuánticos y que permite que dos objetos en ese tipo de estados, denominados entrelazados, puedan, bajo determinadas condiciones, seguir constituyendo un solo sistema, por muy separados en

el espacio-tiempo que lleguen a estar. En consecuencia, se produce una correlación entre los resultados de las medidas conjuntas sobre ellos de algunas propiedades, imposible de justificar para cualquier teoría que conciba la realidad como siempre separable en partes locales, independientes por completo entre sí y con propiedades objetivamente determinadas. Este tipo de correlaciones se suelen denominar correlaciones EPR, o tipo Einstein-Podolsky-Rosen, los nombres de los tres científicos que las analizaron en 1935.

> El mejor conocimiento de un todo no incluye el mejor conocimiento de sus partes.
>
> ERWIN SCHRÖDINGER

La descripción teórica de un par de partículas entrelazadas se corresponde con un estado cuántico general que no admite factorización de una forma separada, es decir, como producto de una función de onda de la partícula 1 por una función de onda de la partícula 2. Para explicar en qué consiste esta imposibilidad matemática, y cuáles son sus consecuencias, vamos a recurrir a los qubits, que como hemos visto se pueden implementar físicamente de diversas maneras. Por ejemplo, sobre un fotón, superponiendo dos estados fundamentales de polarización fotónica. También, por supuesto, podríamos implementar un qubit sobre una partícula de espín 1/2, como una superposición de dos estados cuánticos, hacia arriba y hacia abajo, de la tercera componente $\vec{S}_z$ de su espín.

Supongamos ahora que tenemos dos qubits. Para implementarlos habremos necesitado dos sistemas, por ejemplo, dos fotones, ya que para cada qubit se requiere uno. Esto quiere decir que van a intervenir dos funciones de onda, una para cada qubit o fotón, de forma que introducimos los números 1 y 2 para referirnos a los fotones y poder distinguirlos. Aparecen, pues, dos funciones de onda monofotónicas:

$$\psi(1) = a_1 \cdot \rightarrow_1 + b_1 \cdot \uparrow_1$$
$$\psi(2) = a_2 \cdot \rightarrow_2 + b_2 \cdot \uparrow_2.$$

Una manera directa de escribir a partir de ellas una función de onda para dos fotones, $\Psi(1, 2)$, es calcular su producto; vamos a

simbolizar el producto entre funciones de onda de distintas partículas como ×, para distinguirlo del otro producto introducido (·), que opera entre un número y una función de onda, o entre dos números. Podemos escribir entonces:

$$\Psi(1,2) = \psi(1) \times \psi(2) = (a_1 \cdot \rightarrow_1 + b_1 \cdot \uparrow_1) \times (a_2 \cdot \rightarrow_2 + b_2 \cdot \uparrow_2),$$

una expresión que conduce finalmente, desarrollando todos los productos, a la siguiente función de onda para un sistema de dos qubits:

$$\begin{aligned}\Psi(1,2) = \psi(1) \times \psi(2) &= (a_1 \cdot \rightarrow_1) \times (a_2 \cdot \rightarrow_2) + (a_1 \cdot \rightarrow_1) \times (b_2 \cdot \uparrow_2) + \\ &+ (b_1 \cdot \uparrow_1) \times (a_2 \cdot \rightarrow_2) + (b_1 \cdot \uparrow_1) \times (b_2 \cdot \uparrow_2) = \\ &= (a_1 \cdot a_2) \cdot (\rightarrow_1 \times \rightarrow_2) + (a_1 \cdot b_2) \cdot (\rightarrow_1 \times \uparrow_2) + (b_1 \cdot a_2) \cdot (\uparrow_1 \times \rightarrow_2) + \\ &+ (b_1 \cdot b_2) \cdot (\uparrow_1 \times \uparrow_2).\end{aligned}$$

En esta función de onda para dos fotones —o dos qubits—, cada fotón puede asociarse a una función de onda individual ψ, y el producto de las dos funciones individuales proporciona la función de onda global. Este tipo de funciones de onda representan estados sin entrelazamiento.

¿Cómo son las funciones de onda correspondientes a estados entrelazados? Son aquellas para las que la expresión en forma de producto de funciones de onda individuales no es posible. Por ejemplo, las siguientes cuatro funciones de onda, que representan los denominados *estados de Bell*, en honor al físico John Bell, son estados entrelazados (expresados en términos fotónicos, con el par fundamental de estados de polarización lineal y normalizados):

$$\begin{aligned}\Psi^{\pm}(1,2) &= (1/\sqrt{2}) \cdot [(\rightarrow_1 \times \uparrow_2) \pm (1/\sqrt{2}) \cdot (\uparrow_1) \times (\rightarrow_2)] = \\ &= 1/\sqrt{2} \cdot [(\rightarrow_1 \times \uparrow_2) \pm (\uparrow_1 \times \rightarrow_2)] \neq \psi(1) \times \psi(2)\end{aligned}$$

$$\begin{aligned}\Phi^{\pm}(1,2) &= (1/\sqrt{2}) \cdot [(\rightarrow_1 \times \rightarrow_2) \pm (1/\sqrt{2}) \cdot (\uparrow_1) \times (\uparrow_2)] = \\ &= 1/\sqrt{2} \cdot [(\rightarrow_1 \times \rightarrow_2) \pm (\uparrow_1 \times \uparrow_2)] \neq \phi(1) \times \phi(2).\end{aligned}$$

En términos generales de qubits, las correspondientes expresiones se suelen escribir de una forma abreviada, en la que se

suprimen a la derecha de las ecuaciones los índices 1 y 2 de sistema o partícula:

$$\Psi^{\pm}(1,2) = 1/\sqrt{2}\ [0^{Q} \times 1^{Q} \pm 1^{Q} \times 0^{Q}]$$
$$\Phi^{\pm}(1,2) = 1/\sqrt{2}\ [0^{Q} \times 0^{Q} \pm 1^{Q} \times 1^{Q}].$$

Estos cuatro estados de Bell constituyen un cuarteto fundamental o «base» para todas las funciones de onda correspondientes a un sistema de dos partículas —de dos qubits—, lo que quiere decir que cualquier estado general de ese sistema, entrelazado o no, se puede representar como una superposición o suma de las cuatro funciones de onda dadas (que son entrelazadas y están normalizadas). Los estados de Bell son, además, estados en los que ninguna de las dos partículas tiene determinado el valor de la propiedad correspondiente (polarización, para dos fotones; componente tercera de espín, para dos electrones; etc.), de modo que la medida de esa propiedad sobre una cualquiera de las dos partículas individuales tiene en principio un $100|1/\sqrt{2}|^2 = 50\%$ de probabilidad de producir un resultado u otro, de los dos posibles.

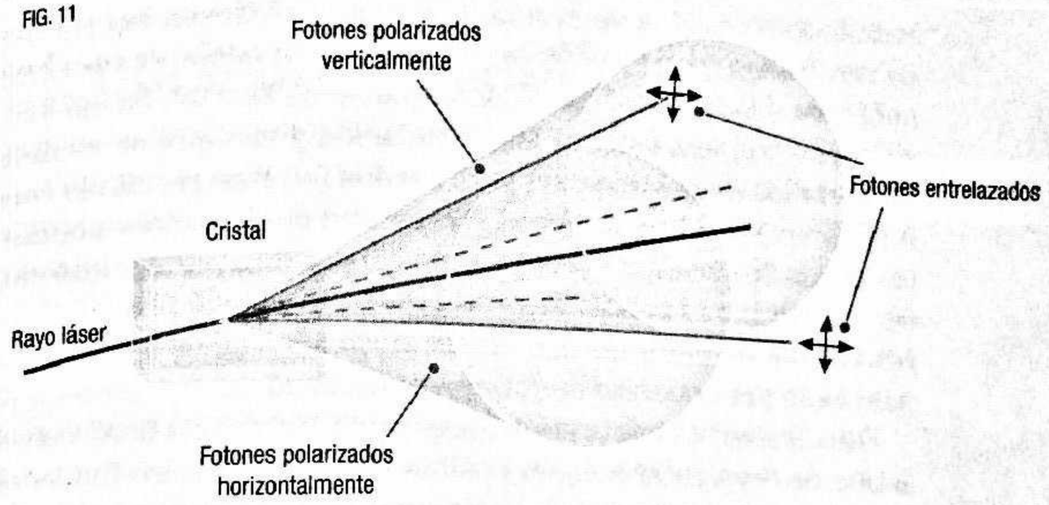
La característica esencial de un estado entrelazado es que las distribuciones de probabilidad para los resultados de las medidas de la correspondiente propiedad, sobre las dos partículas, están trabadas, es decir, se van a obtener resultados correlacionados. De modo que al realizar sobre dos objetos en un estado entrelazado sendas medidas de la propiedad en cuestión, suponiendo que se efectúan en un sistema de referencia dado en el que una de las dos medidas se hace antes que la otra, el resultado de la primera medida condiciona la probabilidad para el resultado de la segunda, algo que no sucede para las funciones no entrelazadas. Existen muchos estados entrelazados de dos partículas, y, en general, en términos de la teoría cuántica de la información, cada uno de los cuatro estados de Bell presenta el máximo de entrelazamiento posible para dos partículas; por supuesto, también existen estados entrelazados de tres y más partículas.

¿Cómo se pueden generar pares de fotones entrelazados? Un procedimiento muy usado es la SPDC (*Spontaneous Optical Pa-*

rametric Down-Conversion, conversión óptica paramétrica, espontánea y a la baja, también denominada fluorescencia paramétrica). Se trata de un fenómeno en el cual, a partir de un fotón primario, que desaparece, se generan —a veces— dos fotones secundarios, con polarizaciones y localizaciones correlacionadas. Para provocar una SPDC, se hace incidir un láser sobre un tipo específico de cristal, como el borato de beta-bario, que permanece inalterado durante el proceso. El fenómeno es espontáneo, de manera que un par de fotones entrelazados se crea solo en algunas ocasiones, al azar, mientras que la mayoría de los fotones atraviesan el cristal sin provocarlo; el proceso, cuando sucede, se considera estimulado por las fluctuaciones cuánticas aleatorias del vacío, unos procesos cuánticos que se generan a partir de la energía siempre presente en el vacío. De la aplicación estricta de los principios de conservación de energía y momento entre los fotones involucrados se deriva un proceso «a la baja» o «descendente», en el sentido de que se producen fotones con energías individuales que han de ser, por conservación de la energía, menores que la del incidente. Además, la conservación del momento impone que los dos fotones de cada par producido se propaguen según direcciones simétricas entre sí en relación con la de incidencia del fotón primario.

Se conocen dos tipos de SPDC; en el tipo I los fotones producidos tienen polarizaciones paralelas entre sí y perpendiculares a la del fotón incidente, mientras que en el tipo II los fotones producidos tienen polarizaciones perpendiculares entre sí, con la de uno de ellos paralela a la del fotón incidente. En la figura 11 se ilustra el tipo II, en el que los dos fotones producidos se emiten sobre dos direcciones situadas sobre sendas superficies de dos conos que no comparten eje, aunque sí vértice, situado en el lugar del cristal donde se originan los fotones. Para cada fotón incidente, pues, hay dos superficies cónicas de direcciones posibles para cada uno de los dos fotones producidos, una por cada modo fundamental de polarización, que en la figura se han indicado como horizontal y vertical. Pues bien, de todos los pares de fotones producidos, en particular los que son localizados según las direcciones de intersección de las dos superficies cónicas (y solo ellos) constituyen

FIG. 11



Proceso SPDC tipo II. Los dos fotones que son localizados según las direcciones de intersección entre las superficies de los dos conos —líneas continuas— han sido producidos en un estado entrelazado. En este estado no solo se superponen los dos estados de polarización posibles, de modo que ninguno de los dos fotones tiene polarización definida, sino que también, y esto es lo crucial, las probabilidades para los resultados de las medidas de la polarización sobre los dos fotones están trabadas: no se pueden considerar como independientes, por mucha separación que se establezca entre ellos.

un par entrelazado. En la figura, esas dos direcciones privilegiadas están marcadas con sendas líneas continuas; en cambio, dos fotones que *aparecen* según, por ejemplo, las dos direcciones marcadas con líneas discontinuas, no están entrelazados.

A partir del proceso SPDC-II, con las operaciones adecuadas sobre cada par entrelazado producido, es posible generar los cuatro estados entrelazados de Bell, usados para muchas aplicaciones en teoría cuántica de la información. La principal peculiaridad de estos estados es que, si sobre cada par de estos fotones entrelazados, en el estado cuántico conjunto descrito por uno cualquiera de los cuatro estado de Bell, se miden sus respectivas polarizaciones, los resultados experimentales muestran una estricta correlación. En efecto: por ejemplo, sobre los estados $\Psi^{\pm}$, ambos fotones resultan siempre con polarizaciones opuestas, no importa cuánto tiempo haya transcurrido ni cuán alejados estén ya entre sí. Es decir, si sobre uno se obtiene el resultado hori-

zontal, sobre su compañero en ese par entrelazado se obtiene el resultado vertical, y viceversa. Y nunca se obtienen las parejas de resultados (→→) y (↑↑): los resultados son siempre opuestos sobre los dos fotones. En los dos estados de Bell Φ^*, en cambio, se produciría una estricta anticorrelación y siempre se mediría igual estado de polarización para los dos fotones: resultado conjunto (→→) o (↑↑), y nunca se encuentran polarizaciones opuestas de los dos fotones. El fenómeno es, por otra parte, aleatorio, de manera que es imposible prever qué combinación concreta de resultados, de entre las dos únicas posibles, vamos a encontrar para cada par concreto de fotones entrelazados.

Para acabar, es importante hacer una advertencia final, con el ánimo de desalentar a algún posible visionario, futuro fundador de una nueva empresa de telecomunicaciones: no es posible desarrollar un sistema de transmisión instantánea de información usando las correlaciones cuánticas EPR. El inherente e ineludible azar, siempre presente, destruye lo que hubiese sido un fantástico recurso. Pero otras muchas aplicaciones fascinantes sí serán posibles, como vamos a ver.

CAPÍTULO 2

Teleportación cuántica

La mecánica cuántica permite una aplicación sorprendente del entrelazamiento: teleportar el estado de un sistema cuántico, es decir, trasladarlo a distancia sin que ni materia ni energía recorran el camino intermedio.

La palabra «teletransporte», atendiendo a su etimología, referiría al fenómeno por el que algo se traslada a distancia. Dicho así, no suena muy revolucionario, pero si se añade la característica de realizar ese transporte entre dos regiones del espacio sin recorrer las zonas intermedias y de forma instantánea, empieza ya a sonar a ciencia ficción… y a violación de la relatividad. Aprovechando el entrelazamiento cuántico, hoy en día se han hecho experimentos de teleportación cuántica, por supuesto respetando a rajatabla los postulados de la teoría de la relatividad. Expliquemos en qué consisten, no sin señalar antes que, aunque la palabra «teleportación» no existe en español, se ha impuesto como término científico aplicado al fenómeno, para hacer hincapié en que los correspondientes experimentos no consisten en transportar energía o materia de un lado a otro.

CLONAR ES POSIBLE... SI NO CONLLEVA DUPLICACIÓN

En primer lugar, reflexionemos sobre que, para tener una réplica idéntica a un objeto dado en otro lugar del espacio, no necesi-

tamos trasladarlo en sí, basta con poder reproducirlo en el otro lugar; es lo que se hace al enviar un fax, por ejemplo. Entonces, ¿qué tiene de revolucionaria la teleportación cuántica? Pues que la copia del objeto, a diferencia de lo que sucede con un fax normal, aparece en un lugar distante sin que haya habido ningún transporte de energía o materia, y de forma que se respetan los axiomas relativistas (por supuesto). Se trata de conseguir que un objeto a distancia adquiera el mismo estado del que tenemos a nuestro lado, y que desconocemos, pero sin que el objeto original se desplace ni duplique, ya que el proceso no lo va a transportar pero sí, irremediablemente, lo va a alterar.

En efecto, la teleportación cuántica presenta además esa diferencia fundamental con el fax ordinario: al producirse el fenómeno, cambia el estado original del sistema, en conformidad con el teorema de no duplicación cuántica, que impide hacer réplicas de un sistema cuántico, cuyo estado desconocemos, sin destruir el original, por los límites que establece el principio de indeterminación. Pero, como vamos a ver, el entrelazamiento EPR va a permitir un proceso de «fax» de un estado cuántico, y además de forma instantánea —pero siempre sin transporte de información superlumínico—, eludiendo el problema principal de que un proceso estándar de escaneo completo sobre un objeto cuántico sea imposible, por el indeterminismo vigente en el mundo cuántico. En cualquier caso, para saber que la teleportación del estado ha sido consumada, se requiere incorporar un canal clásico adicional de transmisión de información, lo que, a la postre, garantiza la imposibilidad de violar los límites relativistas a la transmisión de cualquier señal (la velocidad límite es la velocidad de la luz en el vacío).

Imaginemos que, como primer paso para construir un fax cuántico, queremos extraer la información de un objeto que poseemos y que deseamos duplicar a distancia. Para copiarlo, hay que someterlo a interacciones que nos aporten información completa sobre cuál es su estado. Pero recordemos que un objeto cuántico, en general, se halla en un estado de superposición de numerosas posibilidades, de forma que es la medida —la interacción que supone cualquier procedimiento experimental— la que determina el estado final, de una manera azarosa. En otras palabras: si para copiar un sistema cuántico lo «miramos», esto es, experimentamos sobre él, alteramos sin remedio el original, perdiendo siempre alguna información complementaria a la determinada por nuestras intervenciones. La duplicación exacta es, pues, imposible. Y todo porque en mecánica cuántica la máxima información disponible sobre un estado está, en general, limitada, como consecuencia de las relaciones de indeterminación vigentes para cada dos observables complementarios. Aunque es cierto que se pueden clonar algunos estados fundamentales —por ejemplo, un estado de polarización bien definido, sin superposición—, es imposible construir una máquina de clonar universal, capaz de clonar cualquier estado cuántico arbitrario.

APLICANDO EL ENTRELAZAMIENTO

En 1993, Charles Bennett y otros cinco científicos sugirieron desde las páginas de la revista *Physical Review Letters* usar el entrelazamiento cuántico para realizar una teleportación, con unos procedimientos que fueron realizados en el laboratorio casi un lustro después. Empezaban su artículo, titulado «Teleportando un estado cuántico desconocido mediante la vía dual de un canal clásico y un canal EPR [Einstein-Podolsky-Rosen]», afirmando:

> La existencia de correlaciones de largo alcance entre pares de partículas EPR plantea la cuestión de su uso para la transferencia de información. El mismo Einstein empleó la palabra «telepáticamente» en este contexto. Es bien conocido que la transferencia instantánea de información es definitivamente imposible. Aquí mostramos que las correlaciones EPR pueden sin embargo intervenir en la «teleportación» de un estado cuántico inalterado, de un lugar a otro, por un remitente que no conoce ni el estado que se va a teleportar ni el lugar donde está quien se pretende que lo reciba.

Es conocido que la transmisión instantánea de información es definitivamente imposible. No obstante, las correlaciones EPR permiten «teleportar» un estado cuántico intacto desde un lugar a otro.

Charles Bennett

El protocolo teórico que propusieron, por completo novedoso en ese momento, consistía en la ejecución de un fenómeno de teleportación de un estado cuántico, pero no de materia o radiación; no obstante, y como es obligado en el formalismo cuántico, no se producía la duplicación final del estado cuántico teleportado, pues es inevitable que en el proceso se destruya el original. Aunque podría creerse que una propuesta teórica tan audaz tardaría en verse culminada en la práctica, lo cierto es que solo casi cinco años más tarde se realizaban dos experiencias independientes de teleportación, sobre una distancia de algunos pocos metros y por técnicas distintas. Una se culminó en Innsbruck y otra en Roma, de la mano de sendos equipos de investigadores dirigidos, respectivamente, por Anton Zeilinger y Francesco de Martini.

El experimento de Innsbruck, realizado en 1997, siguió más fielmente la propuesta original de Bennett, teleportando el estado de polarización de un fotón; en lo que sigue, vamos a describir con detalle un esquema similar al que realizaron. Para empezar, y puesto que los vamos a necesitar como ingredientes teóricos esenciales de la teleportación, recordemos en primer lugar que el estado general que representa en física cuántica la polarización de un fotón (que vamos a etiquetar como fotón 1), tiene una expresión que es superposición o suma de dos estados fundamentales, por ejemplo, uno de polarización horizontal, →, y otro de polarización vertical, ↑. Es decir, que el estado cuántico general de polarización de un fotón con índice de partícula 1 se corresponde con la suma o combinación:

$$\Psi(1) = a \cdot \rightarrow_1 + b \cdot \uparrow_1$$

donde los números $|a|^2$ y $|b|^2$ representan, respectivamente, las probabilidades de que, al hacer que el fotón atraviese un medi-

dor de polarización, como un cristal de calcita, el resultado sea horizontal o vertical. Debido a esta interpretación, la suma de estos dos números debe ser 1, una condición que se dice que «normaliza» la distribución de probabilidades. En segundo lugar, recordemos que un estado entrelazado de dos fotones, etiquetados respectivamente como 2 y 3, puede ser, por ejemplo, el estado de Bell $\Psi^-(2,3)$, que es un estado de máximo entrelazamiento representado por la expresión:

$$\Psi^-(2,3) = 1/\sqrt{2}\,(\rightarrow_2 \times \uparrow_3 - \uparrow_2 \times \rightarrow_3).$$

Como ya sabemos, en este estado de superposición ninguna de las dos partículas se asocia con un valor definido del observable polarización: tanto el fotón 2 como el 3 aparecen ligados a las dos polarizaciones, horizontal y vertical. Además, la medida conjunta —sobre los dos fotones a la vez— de sus respectivas polarizaciones, por las características del entrelazamiento, presentará una correlación perfecta: si sobre el fotón 2 se obtiene el resultado →, sobre el 3 se obtiene ↑, y viceversa, con independencia de lo alejados que estén entre sí. Cada intervención experimental de este tipo se denomina *medida conjunta no local estocástica*, en el sentido no de que la medida sobre un fotón influencie causalmente el resultado de la medida sobre su compañero, nada de eso —¡sería una violación de la relatividad!—, sino de que las dos medidas, producidas la una respecto a la otra bien antes, bien después, o al mismo tiempo, según el sistema de referencia concreto elegido, siempre muestran la correlación que predice la función de onda entrelazada del sistema. El adjetivo *no local* expresa que esta correlación es independiente de la distancia mutua a que se encuentren los dos fotones, y el término *estocástico* indica que para cada par de fotones podemos encontrar por azar como resultado una de las dos siguientes posibilidades: polarización horizontal para el fotón 2 y polarización vertical para el fotón 3; o bien, resultados intercambiados (y nunca resultados iguales). Si realizamos la medida sobre un número suficiente de pares de fotones, todos preparados igual-

mente en el estado entrelazado de Bell $\Psi^-(2, 3)$, la estadística final de resultados ofrecerá un 50% de resultados para cada posibilidad de las dos enunciadas.

Supongamos para empezar que una observadora a la que llamaremos Alicia tiene un fotón 1, en un estado general de polarización superpuesta horizontal y vertical, es decir:

$$\psi(1) = a \cdot \rightarrow_1 + b \cdot \uparrow_1,$$

que desconoce (no sabe los valores de los números a y b) y que no puede medir, pues solo lograría determinarlo en su polarización, alterándolo irremediablemente y perdiendo para siempre parte de la información disponible con anterioridad a su medida. Además, se dispone de una fuente que genera los fotones 2 y 3 en el estado entrelazado de Bell $\Psi^-(2, 3)$, teniéndose que el fotón 2 se lo queda Alicia y el 3 viaja hasta un segundo observador, al que llamaremos Blas, esté él donde esté (el fotón 3 sí que recorre la correspondiente distancia, por ejemplo por una fibra óptica o por una transmisión aérea). La experiencia va a consistir en una serie de maniobras en la que se van a entrelazar entre sí los fotones, lo que culminará con el resultado de que el fotón 3, ya situado a una distancia arbitraria del 1, y sin que Alicia necesite conocer dónde está, se habrá convertido —solo a veces— en la réplica del fotón 1 original, es decir, en un fotón con el mismo estado cuántico en que estaba el 1 al empezar el procedimiento. Pero entonces el fotón 1 siempre habrá cambiado de estado, así que no se va a producir una duplicación, tan solo la teleportación de un estado cuántico. En concreto, se va a teleportar el estado cuántico del fotón 1 sobre el fotón 3.

Así pues, suponemos que Alicia, que se encuentra en el lugar L1, desea que Blas, en un lugar L2, tenga un fotón con igual estado de polarización que el fotón 1 que ella tiene, pero que desconoce, porque si lo midiera solo lograría determinarlo hacia una polarización, hacia un estado colapsado, distinto al inicial. Repárese en que «conocer el estado de polarización del fotón» en mecánica cuántica significa conocer los valores de los dos números a y b, pero solo en el caso de que el fotón 1 estuviera en

uno de los dos estados fundamentales, horizontal ($a=1$, $b=0$) o vertical ($a=0$, $b=1$), sería posible averiguarlo y duplicarlo —ahora sí— fácilmente. Para ello bastaría con emplear el medidor de polarización adecuado (un cristal de calcita, por ejemplo), determinar su estado, comunicárselo a Blas por cualquier tipo de canal y este podría replicarlo sin problemas, en cualquier lugar. Algo que es imposible para el estado general, suma o combinación de polarizaciones.

Cada realización del experimento comienza preparando un par de fotones (2 y 3) entrelazados en el estado de Bell $\Psi^-(2, 3)$, algo de lo que se puede encargar la misma Alicia o un colaborador, al que llamaremos Luis, situado en un lugar L3 cualquiera; uno de los fotones, el 2, se pone a disposición de Alicia, y el 3 se le entrega a Blas. Por supuesto, hay que garantizar que se preserve el entrelazamiento entre ellos, algo que no es fácil: cualquier interacción con el entorno desplomaría la superposición, produciéndose el colapso de la función de onda y el fracaso de la experiencia. Y es que el fenómeno de la denominada *decoherencia*, las interacciones fortuitas con el entorno que desploman las superposiciones cuánticas, es siempre una de las grandes amenazas a evitar en estos procesos.

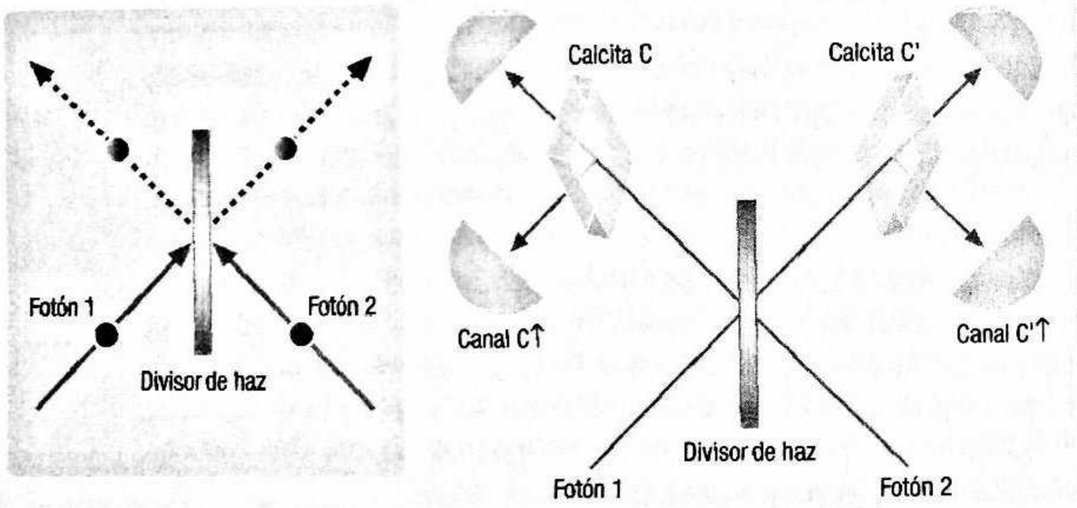
A continuación, Alicia va a entrelazar los fotones 1 y 2. Para ello, realiza una experiencia en la que los lanza a la vez contra un divisor de haz, un tipo de operación que se conoce como medida de Bell, ya que el resultado es que los dos fotones resultan entrelazados, en uno de los cuatro estados de Bell. El dispositivo que utiliza se ilustra en la figura 1, a la derecha; consta de un divisor de haz o espejo semirreflector (ampliado a la izquierda en la misma figura), incidiendo cada fotón sobre uno de sus dos lados; tras los dos canales de salida se colocan sendos prismas polarizadores, C y C' —por ejemplo, dos cristales de calcita—, y, tras cada uno de ellos, dos fotodetectores, uno por canal de salida: horizontal, H, y vertical, V. Cuando Alicia lanza los dos fotones sobre el divisor de haz, el resultado de esta operación es que, a su salida, los dos fotones 1 y 2 pasan a ocupar uno de los cuatro estados de Bell, con igual probabilidad (del 25%) para cada uno de ellos. La situación que se va a plantear a continuación será,

pues, cómo discriminarlos, para lo que van a intervenir los cuatro fotodetectores dispuestos.

El formalismo teórico cuántico establece que el estado del sistema único compuesto por los tres fotones, tras la operación de Alicia y antes de la medida en los correspondientes fotodetectores, viene descrito por la siguiente función de onda, superposición general cuántica de cuatro resultados posibles:

$$\Psi(1,2,3)=\psi(1)\times\Psi^{-}(2,3)=$$
$$=(a\cdot\rightarrow_1+b\cdot\uparrow_1)\times(1/\sqrt{2})\cdot[(\rightarrow_2\times\uparrow_3)-(\uparrow_2\times\rightarrow_3)]=$$
$$=(a/\sqrt{2})\cdot[(\rightarrow_1)\times(\rightarrow_2)\times(\uparrow_3)]-(a/\sqrt{2})\cdot[(\rightarrow_1)\times(\uparrow_2)\times(\rightarrow_3)]$$
$$+(b/\sqrt{2})\cdot[(\uparrow_1)\times(\rightarrow_2)\times(\uparrow_3)]-(b/\sqrt{2})\cdot[(\uparrow_1)\times(\uparrow_2)\times(\rightarrow_3)]=$$
$$=\Omega_A(1,2,3)+\Omega_B(1,2,3)+\Omega_C(1,2,3)+\Omega_D(1,2,3).$$

FIG. 1



Los dos fotones 1 y 2 inciden a la vez sobre un divisor de haz 50:50 (izquierda), sobre el cual cada fotón tiene un 50% de probabilidades de reflejarse y otro 50% de transmitirse. Convenientemente lanzados, dos fotones indistinguibles que llegan de manera simultánea al espejo tienen un 25% de probabilidades de alcanzar después, también simultáneamente, sendos detectores dispuestos tras diferentes cristales de calcita (derecha), esto es, de producir en ellos posteriormente «detección en coincidencia». Del 75% de las veces restantes, hay un 50% en las que solo un detector de los cuatro da señal, ya que los dos fotones acaban en él, y un 25% en las que los dos fotones acaban de nuevo en detectores distintos, pero ahora tras la misma calcita.

Los cuatro estados Ω que aparecen sumados en la superposición cuántica que establece la última igualdad tienen las siguientes expresiones, en términos de los productos de un estado de Bell para los fotones 1 y 2 y una función de onda individual para el fotón 3 (para comprobarlo, basta con sustituir las correspondientes fórmulas para esos cuatro estados de Bell, proporcionadas en el capítulo anterior, y operar, incorporando todas las cancelaciones o *interferencias destructivas* que se dan al desarrollar los productos de cada estado de Bell por la correspondiente función de onda individual):

$$\Omega_A(1,2,3)=(-1/2)\cdot[\Psi^{-}(1,2)\times(a\cdot\rightarrow_3+b\cdot\uparrow_3)]$$
$$=(-1/2)\cdot[\Psi^{-}(1,2)\times\psi(3)]$$
$$\Omega_B(1,2,3)=1/2\cdot[\Psi^{+}(1,2)\times(b\cdot\uparrow_3-a\cdot\rightarrow_3)]$$
$$\Omega_C(1,2,3)=1/2\cdot[\Phi^{-}(1,2)\times(a\cdot\uparrow_3+b\cdot\rightarrow_3)]$$
$$\Omega_D(1,2,3)=1/2\cdot[\Phi^{+}(1,2)\times(a\cdot\uparrow_3-b\cdot\rightarrow_3)].$$

Si examinamos el primer sumando en la expresión obtenida, la función de onda $\Omega_A(1,2,3)$, vemos que corresponde al caso en que el fotón 3, el que tiene Blas, está justo en el estado original Ψ que tenía el fotón 1 antes de que Alicia lo manipulara. En otras palabras: ¡los dos estados sombreados son iguales! De modo que, cuando la función de onda global $\Psi(1,2,3)$ colapse hacia ese estado Ω_A —lo que sucede en un 25% de las realizaciones experimentales—, podrá afirmarse que ha tenido lugar la teleportación de ese estado fotónico individual Ψ, desde el fotón 1, que permanece siempre con Alicia, en el lugar L1, hasta el fotón 3, que está junto a Blas, en el lugar L2.

Por tanto, la predicción teórica cuántica para un esquema experimental como el de la figura 1 se puede resumir afirmando que hay cuatro resultados finales posibles para el experimento, y que cada uno de ellos viene representado por una función de onda global $\Omega(1,2,3)$. La correspondencia entre cada uno de estos cuatro posibles estados Ω con las señales que dan los detectores en cada realización experimental, detectores que señalan cuándo la superposición $\Psi(1,2,3)$ colapsa hacia uno de sus sumandos Ω, puede demostrarse (no es trivial) que se establece de la siguiente forma:

— Cuando los dos fotones 1 y 2 son registrados con polarizaciones opuestas en sendos detectores tras distintos cristales de calcita, es decir, bien en la pareja de detectores CH-C'V, bien en CV-C'H, significa que el estado final conjunto de los tres fotones es $\Omega_A(1, 2, 3)$ (la función de onda Ψ^- predice resultados siempre opuestos para las polarizaciones de los dos fotones). Esta situación ocurre un 25% de las veces y permite elaborar retrospectivamente un relato «clásico» sobre cuál ha sido el camino recorrido por cada fotón desde el divisor de haz hasta los dos detectores. Según este relato (ajeno a la física cuántica, pero muy útil para que los cerebros humanos puedan elaborar imágenes mentales explicativas de los fenómenos), cada fotón ha llegado a «su» detector por un prisma diferente. En cualquier caso, el fenómeno concluye con los dos fotones en estados correspondientes a polarizaciones opuestas, y la teleportación ha sido culminada: Blas posee el fotón 3 en el mismo estado que tenía el fotón 1 de Alicia antes de empezar el proceso (y Alicia lo ha perdido, ya que su fotón 1 acaba en otro estado diferente al inicial, de forma que no ha habido clonación).

— Cuando los dos fotones son registrados de nuevo cada uno en un detector distinto, pero ahora ambos tras uno de los dos cristales de calcita, bien en la pareja de detectores CH-CV, bien en C'H-C'V, significa que el estado final conjunto de los tres fotones es $\Omega_B(1, 2, 3)$. De forma que, en este caso, el relato clásico sobre el camino recorrido por cada fotón, elaborado en retrospectiva, afirmaría que ambos han atravesado el mismo prisma. El evento experimental finaliza, en esta ocasión, resultando de nuevo los dos fotones 1 y 2 en estados con polarizaciones opuestas, posibilidad que ocurre otro 25% de las veces. Una vez que Alicia sabe que en este experimento concreto el estado final ha sido $\Omega_B(1, 2, 3)$, solo tiene que comunicárselo a Blas, por un canal clásico, como un correo o una llamada telefónica. Cuando Blas lo sepa, la teleportación (que ahora ya no será inmediata) requerirá de una última operación adicional: que Blas actúe sobre su fotón 3, que está en el estado de polarización $\Psi'(3) = b \cdot \uparrow_3 - a \cdot \rightarrow_3$, y lo cambie hacia el Ψ original que tenía el 1, es decir, consiga llevar su fotón 3 hacia el estado $\Psi(3) = a \cdot \rightarrow_3 + b \cdot \uparrow_3$. Existen en óptica dispositivos capaces de generar estos cambios, que no son sino giros y cambios de signo en la polarización, así que Blas solo ha de hacer pasar su fotón por el dispositivo adecuado para conseguir, por fin, tener un fotón réplica del inicial —el fotón 1— que Alicia tenía (y que ya no tiene en ese estado, porque ha resultado alterado en el proceso). Puede usar, por ejemplo, una lámina de media onda, un dispositivo óptico que desfasa o retrasa entre sí las dos componentes perpendiculares de polarización fotónica.

— El restante 50% de las veces, los dos fotones son registrados en el mismo detector, que puede ser con igual probabilidad cualquiera de los cuatro, y solo se puede afirmar que el estado final es bien $\Omega_C(1, 2, 3)$, bien $\Omega_D(1, 2, 3)$, con igual probabilidad para cada uno. Estos casos, en que los dos fotones acaban en el mismo estado de polarización final, van a ser los casos fallidos en este protocolo, ya que no se va a poder ultimar la teleportación de estado deseada.

Resumiendo: solo si Alicia observa que con su medida de Bell ha logrado un estado final $\Omega_A(1, 2, 3)$, esto es, cuando los correspondientes detectores CH y C'V, o CV y C'H, señalan a la vez, entonces Blas tiene ya el fotón 3 en un estado réplica del que tenía originalmente el fotón 1 (el cual a su vez ha cambiado, de manera que hay réplica pero no duplicado). Pero obsérvese que Blas no lo puede saber, porque se encuentra en el alejado lugar L2, y el resultado de la medida de Bell es azaroso y nadie puede predecir *a priori* cuándo va a obtenerse esa teleportación directa, que solo ocurre en el 25% de los casos (insistimos: no hay manera de construir un «teléfono cuántico» que transmita información de forma instantánea). Aquí es donde se necesita que intervenga un canal clásico: a través de él, Alicia ha de in-

formar a Blas si ya tiene la réplica de su fotón o no. Es por esto por lo que muchos no aceptan que pueda hablarse de teleportación «instantánea» ni siquiera en las ocasiones en que Blas no debe hacer nada sobre su fotón, porque ya tiene uno en el estado en que estaba el original que tenía Alicia: no la ha habido si se considera que la teleportación solo se ha culminado cuando una información se ha transmitido efectivamente, y esto únicamente sucede cuando el receptor ya la conoce. De modo que, en definitiva, se ha de esperar siempre la información que viaja por el canal clásico.

> Hay que enfatizar que si quien ha preparado el estado a teleportar no le dice a Alicia cuál es, entonces ella no puede de ninguna manera averiguar de qué estado se trata.
>
> **Francesco de Martini**

Como hemos visto, con este montaje experimental solo el 25% de las veces se consigue una teleportación directa. En la práctica, no obstante, la tasa de éxito es siempre inferior, porque hay que tener presente la cruda realidad del laboratorio: los detectores fallan en ocasiones y dejan escapar fotones sin registrarlos; otras veces los dos fotones no llegan con la adecuada sincronización, etc. Del teórico 75% restante, todavía se puede lograr el éxito en un 25% adicional de las ocasiones, aquellas en que Alicia observa, a partir de los dos detectores distintos que señalan tras el mismo prisma, que con su medida de Bell ha logrado un estado final $\Omega_B(1, 2, 3)$, casos en los que para lograr consumar la teleportación Blas debe realizar una operación adicional sobre su fotón 3. Lo puede hacer en cuanto Alicia le informe, por el canal clásico, de que están en ese caso; de esta forma, se logra la teleportación, aunque con retraso. ¡Y todo ello sin que Alicia ni Blas sepan cuál es ese estado! Es decir, sin tener que disponer de la información de cuáles son los valores de las constantes a y b que especifican $\Psi(1)$.

Esta última observación podría sembrar cierta desconfianza en el logro proclamado... Porque, si no saben qué estado han teleportado, ¿cómo pueden estar seguros de que lo han logrado? ¿Cómo pueden aseverar que han satisfecho el requisito de fidelidad o coincidencia plena entre el estado del fotón que

ahora tiene Blas y el que tenía al principio el fotón de Alicia? ¿Solo porque lo dicen las matemáticas de la mecánica cuántica? No, no solo por eso, también porque puede comprobarse en la práctica: basta con proceder con muchos fotones preparados inicialmente de igual forma, esto es, fotones individuales colocados por los mismos procedimientos experimentales en el mismo estado (pero recordemos que en mecánica cuántica, la correspondiente información «máxima» que puede conocerse sobre un estado no lo es tanto como se entendería en física clásica, al estar limitada por las relaciones de indeterminación, de manera que «el mismo estado» refiere a una información fundamentalmente limitada). Por ejemplo, se van teleportando muchos fotones que comparten el mismo estado de polarización, ahora conocido por los investigadores. Se procede a intentar (no siempre se logra) teleportarlos (sus estados), uno tras otro, hasta que Blas pueda reunir el número suficiente de fotones réplica como para poder comprobar, a partir de variados experimentos sobre ellos y las distribuciones de probabilidad de sus resultados, que la polarización del supuesto estado réplica coincide con la del estado preparado en origen. De este modo se determina, además, la fidelidad que se está consiguiendo en el experimento: qué porcentaje de las veces que el formalismo predice el éxito, realmente se ha conseguido (el supuesto estado réplica lo es en efecto). El test se debe realizar para varios tipos distintos de polarizaciones, ya que, por ejemplo, la eficiencia de los detectores varía también con el tipo de polarización de los fotones.

De esta forma, con el diseño expuesto, con dos prismas de calcita incorporados, la eficiencia final teórica del procedimiento es del 50%, que son las veces que teóricamente se debería lograr teleportar un qubit (implementado como el estado general de polarización del fotón 1 y teleportado sobre el fotón 3). Cada experimento ha requerido el uso de dos qubits máximamente entrelazados (los dos fotones 2 y 3 inicialmente entrelazados en un estado de Bell) y dos bits clásicos, acarreando la información que Alicia debe mandar por el canal clásico para que Blas sepa en qué caso están: un bit para comunicar si éxito (el 50% de las veces en que

se logra la teleportación) o fracaso, y otro para que Blas sepa si tiene todavía que transformar su fotón o no. Por supuesto, la fidelidad teórica del 100% en ese 50% de las veces no se alcanzará, por las limitaciones y deficiencias prácticas usuales.

Resumiendo: la teleportación lo es de un estado cuántico, pero no hay transmisión de materia o energía a distancia. Tampoco hay violación de la relatividad: no hay transmisión instantánea o a velocidad superlumínica de información. Se teleporta el estado cuántico en general ignoto de un sistema, destruyendo el original, y se requiere una transmisión por un canal clásico para conocer si el experimento puede darse como concluido con éxito (25% de las veces), pendiente de alguna operación adicional para culminarlo (25% de las veces), o fracasado (50% de las veces), con porcentajes referidos al montaje descrito, con dos prismas de calcita (o dispositivos similares). La teleportación se culmina sin que haya necesidad de que Alicia conozca ni el estado que se transfiere —es más, si no lo conoce, es imposible que lo pueda averiguar, a no ser que haya sido preparado por alguien y este le pase la información— ni el lugar a donde se transfiere (allí donde está Blas).

TELEPORTANDO EXPERIMENTALMENTE

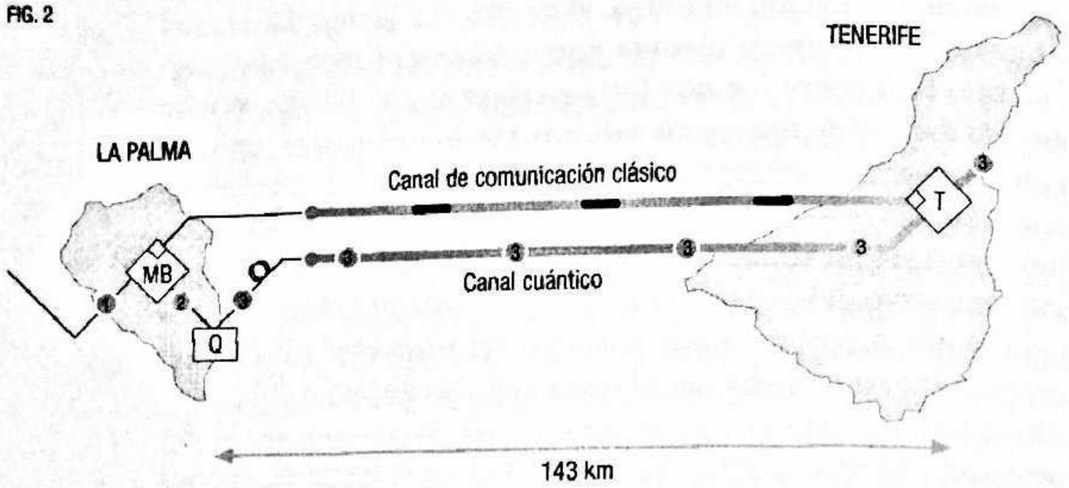
La primera realización experimental siguiendo el tipo de procedimiento anterior se llevó a cabo en Innsbruck, en 1997, sobre una distancia de unos pocos metros (en realidad, uno más simplificado, sin prismas polarizadores, lo que reducía la tasa de éxito a solo el 25%). A partir de ese momento, esa distancia se fue aumentando, así como la eficiencia o tasa de éxito de los experimentos y la fidelidad alcanzada, conforme se iban mejorando y desarrollando nuevos protocolos para la depuración de los inevitables errores y la prevención de la implacable decoherencia (nombre que, como ya hemos dicho, se da al fenómeno en el que las interacciones no controladas del sistema con su entorno provocan colapsos, destruyendo los estados superpuestos y el entrelazamiento).

Respecto al experimento pionero de 1997 llevado a cabo por el equipo de De Martini en Roma, el montaje aplicado difería del de Innsbruck en que la medida conjunta que realiza Alicia no es de tipo Bell sobre los dos fotones (cuando se lanzan ambos sobre un divisor de haz), sino que, a partir de una sugerencia de Sandu Popescu, involucraba la determinación de dos informaciones relacionadas con un mismo fotón: la polarización y el camino recorrido en el montaje, un concepto asociado en el usual relato narrativo del experimento que se construye «hacia atrás» en el tiempo, a partir de una observación posterior (el camino recorrido «en retrospectiva», al que aludimos antes).

Otros hitos de teleportación fotónica —con fotones, no de fotones— se han ido sucediendo desde entonces: en 2004, récord de 600 metros, realizándose una teleportación bajo las aguas del Danubio, de orilla a orilla, empleando fibra óptica; en 2010, teleportación sobre una distancia de 16 km y transmisión al aire libre, algo que se considera un avance fundamental de cara a establecer en el futuro una red cuántica de comunicaciones vía satélite. En 2012 se realizaron dos experimentos también con transmisión de fotones al aire libre, uno en Shanghái, con teleportación de los estados de unos 1 100 fotones en cuatro horas y sobre 97 km, a través de un lago; otro, en el mismo año, con teleportación sin fibra entre las islas de La Palma y Tenerife (Canarias), sobre 143 km, financiado por la Agencia Espacial Europea, ESA (el esquema de esta experiencia se muestra en la figura 2; el que emplearan transmisión fotónica al aire libre se consideró un importante paso hacia la comunicación vía satélite). En 2015 en Estados Unidos, el equipo investigador de Hiroki Takesue llevó a cabo una teleportación sobre 100 km, esta vez usando fibra óptica y con la novedad del uso de unos detectores de radiación monofotónica, hechos con nuevos materiales superconductores, que aumentaban drásticamente la eficiencia de detección en la banda de frecuencias requerida.

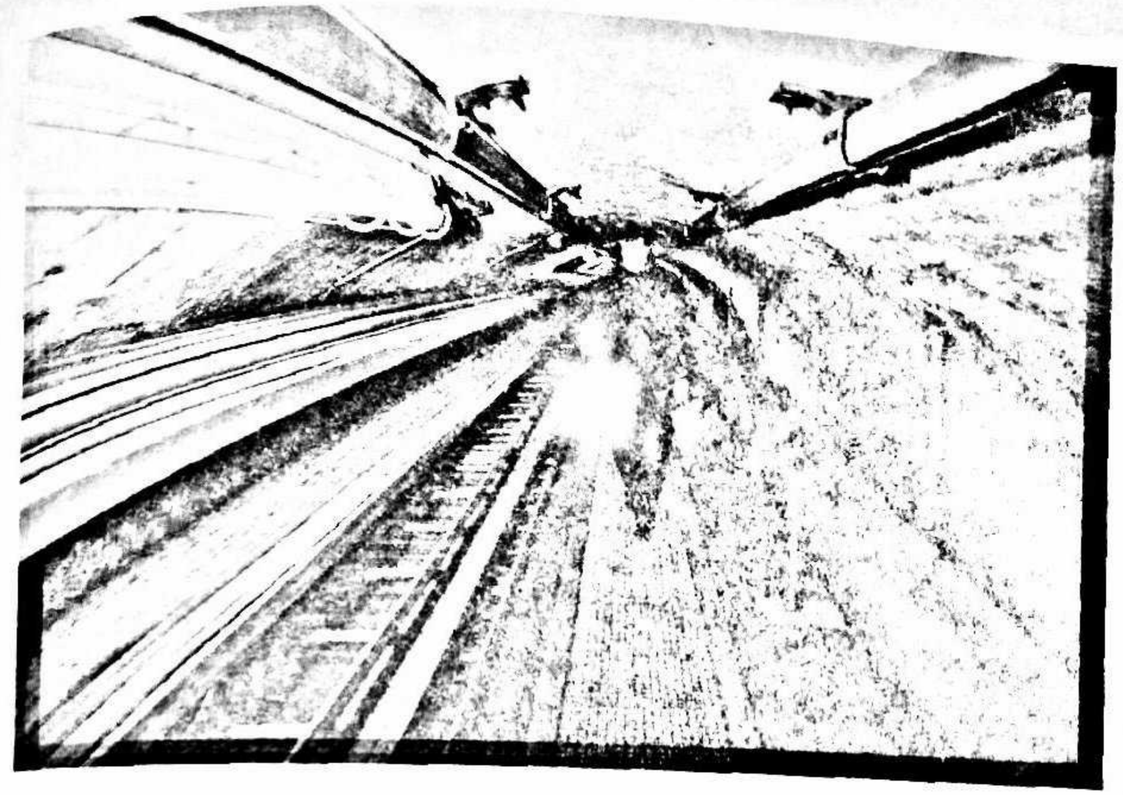
Cerramos esta selección con otros logros recientes: en 2015, en China, una teleportación de un estado que codifica información correspondiente simultáneamente a dos propiedades diferentes de un fotón, por parte de los investigadores Chaoyang

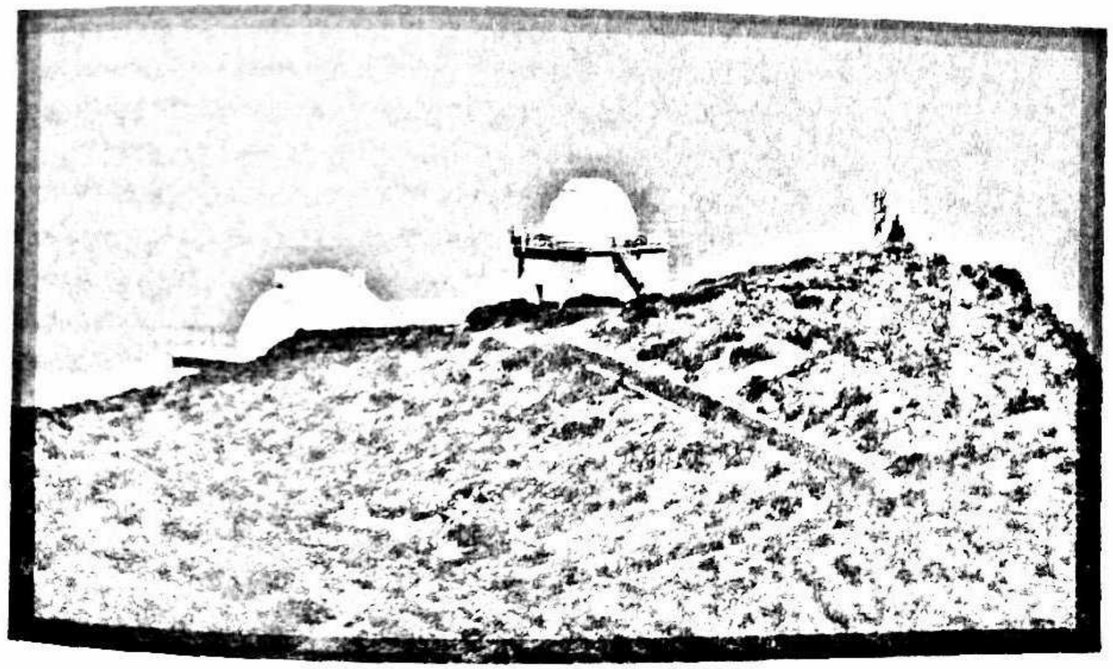
FIG. 2



Experimento de teleportación realizado en 2012 entre el telescopio Jacobus Kapteyn, en la isla canaria de La Palma, y la Estación Óptica Terrestre de la Agencia Espacial Europea (ESA) en Tenerife, en una colaboración de investigadores de varios países europeos. Los fotones 2 y 3 se entrelazaron en un lugar (Q) de La Palma; mientras que el 2 permaneció en esa isla, donde fue sometido a una medida conjunta de Bell (MB) con el fotón 1, el fotón 3 viajó hasta Tenerife mediante transmisión aérea, siendo recogido por un telescopio (T) de la ESA. Cuando la teleportación culminaba con éxito, el estado final de este fotón 3 coincidía con el que tenía inicialmente el 1.

Lu y Jian-Wei Pan. El equipo de este último, en 2016, publicó también una teleportación usando la red urbana de fibra óptica de la ciudad china de Hefei, un avance decisivo hacia la realización futura de un «internet cuántico». En una línea similar y casi simultáneamente, esta vez con la red de fibra de la ciudad canadiense de Calgary, Wolfgang Tittel y otros investigadores realizaron una teleportación a una distancia de unos 8,2 km. Si en Calgary se empleó la red de fibra comercial estándar, en la que se interrumpió cualquier otra transmisión para el experimento, en Hefei hicieron uso de una red de fibra ideada ex profeso para su uso en información cuántica, diseñada, pues, a propósito para minimizar las interferencias de este tipo de señales. En la mayoría de estos experimentos se consiguieron elevadas tasas de fidelidad o correcta reproducción de la información, con una eficiencia o ratio de éxito en el experimento cercana a la teórica.





Arriba, un físico recorre un túnel excavado bajo el río Danubio, durante el experimento en el que se logró por primera vez una teleportación a 600 m de distancia. Abajo, en primer término, el telescopio Jacobus Kapteyn, que recogió la señal fotónica aérea en la teleportación de las islas Canarias en 2012.

Teleportando con materia

Hasta ahora hemos hablado de fenómenos de teleportación realizados con fotones. ¿Es posible experimentar de forma similar con partículas materiales, como los átomos? Bien entendido que siempre se teleporta «sobre», es decir, hay transferencia no de las partículas, sino de su estado cuántico. Porque hay que reconocer que, dada las peculiaridades de los entes fotónicos, esa luz tan diferente a la más «vulgar» materia, un fenómeno cuántico como la teleportación tal vez podría despertar incluso más sorpresa si se realizara sobre objetos materiales. Pues bien, hoy en día también se han realizado ya numerosos fenómenos de teleportación con átomos, e incluso mixtos o *interespecies*, en los que las entidades original y receptora de la información cuántica o estado teleportado no tienen la misma naturaleza. Para ilustrarlo, vamos a mencionar solo algunos de ellos. En 1998, por ejemplo, Michael Nielsen y su equipo implementaron en Los Álamos una teleportación del estado cuántico de un núcleo de carbono, integrante de un sistema de dos núcleos entrelazados, hacia un núcleo de hidrógeno, a partir de un fenómeno de resonancia magnética nuclear (una teleportación interespecies materiales). En 2004, un grupo de investigadores de Innsbruck dirigido por Mark Riebe publicó en la revista *Nature* un experimento de teleportación de un estado cuántico entre un par de iones de calcio encerrados en una trampa de iones, dispositivo en el que se capturan iones confinándolos en una región del espacio, mediante una combinación de campos electromagnéticos. De forma análoga al procedimiento aquí expuesto para los fotones, el equipo de Riebe teleportó el estado de un ion del par entrelazado sobre su compañero, situado a una distancia de unos pocos metros.

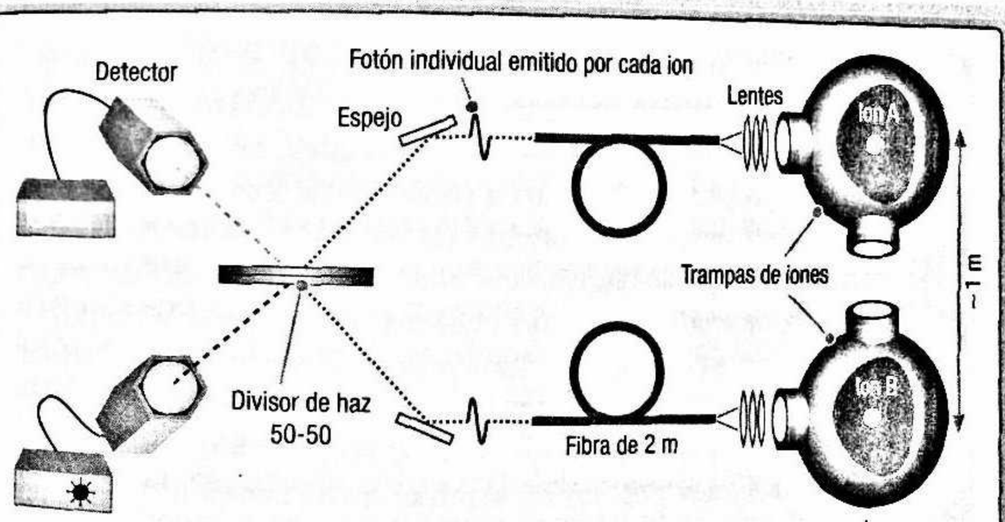
Poco después, en 2006, un equipo dirigido por Eugene Polzik realizó, en el Instituto Niels Bohr de Copenhague, la primera teleportación interespecies entre luz y materia. Siguiendo una propuesta experimental de Ignacio Cirac y Klemens Hammerer, se transfirió el estado de un pulso de radiación integrado por unos pocos fotones sobre un conjunto de 10^{12} átomos de cesio, haciendo uso de un entrelazamiento creado entre el conjunto de átomos

TELEPORTANDO ENTRE ÁTOMOS ATRAPADOS

Las trampas de iones juegan un papel esencial en la construcción de ordenadores cuánticos. Por ello, y cara a la implementación de memorias cuánticas, es importante realizar también experimentos de teleportación entre átomos atrapados.

Una teleportación entre átomos distantes

En 2004, dos equipos independientes lograron teleportar un qubit atómico usando iones atrapados, de berilio en un caso y de calcio en el otro. En 2009, un equipo del JQI (*Joint Quantum Institute*, Universidad de Maryland) realizó una teleportación entre dos átomos de iterbio confinados en sendas trampas separadas un metro entre sí, consiguiendo una fidelidad media del 90 %. Según se ilustra en la imagen, cada ion fue aislado en una trampa en la que se aplicó un alto grado de vacío, quedando los iones suspendidos, como «enjaulados», en una celda invisible creada mediante los campos electromagnéticos, y rodeados por electrodos metálicos. Cada ion puede situarse en dos estados de energía, de modo que el qubit se implementa como un estado superposición de ambos. Los experimentadores, a partir de los fotones emitidos por los átomos al ser excitados mediante pulsos láseres, lograban entrelazar los iones, es decir, colocar los dos qubits atómicos en un estado entrelazado, a partir del cual culminaban la teleportación. Este diseño experimental, al combinar fotones —ideales para la transmisión rápida de información a medias distancias— y átomos —adecuados como soporte físico para construir memorias cuánticas estables—, resultaba idóneo como base de una arquitectura para un futuro «repetidor cuántico». La teleportación cuántica de información constituiría entonces el recurso que permitiría desarrollar un «internet cuántico».



Cada ion permanece aislado en una trampa de alto vacío. Sobre el ion A se consigue almacenar un qubit de información, que es teleportado sobre el ion B, vía el entrelazamiento de ambos y la posterior emisión de sendos fotones que, conducidos por fibras ópticas, se hacen interferir antes de su detección.

y otro pulso auxiliar de radiación. En este experimento, publicado también en *Nature*, se consiguió una fidelidad del 60%. En 2009, el equipo de Steven Olmschenk publicó, esta vez en *Science*, un experimento, realizado en el JQI (*Joint Quantum Institute*, de la Universidad de Maryland), en el que un qubit almacenado sobre un ion de iterbio en una trampa era teleportado sobre un segundo átomo, situado en otra trampa a un metro de la del primero. Este logro, afirmó Christopher Monroe, uno de sus autores, «encierra un gran potencial para establecer la base de un esquema de "repetidor cuántico", que permita construir una red de memorias cuánticas extendiéndose sobre grandes distancias».

A partir de 2010, merece la pena destacar en primer lugar el experimento realizado en 2012 por el equipo de Xiao-Hui Bao, en Hefei, China, en el que se efectuó una teleportación entre dos objetos macroscópicos, compuestos ambos por un conjunto de átomos de rubidio, sobre una distancia de unos 150 m, usando fotones entrelazados auxiliares. Y para acabar nuestra pequeña lista, en 2014 el equipo de Nicolas Gisin, en Ginebra, teleportó un estado fotónico sobre un ion en un cristal a 25 km de distancia, con fibra óptica. Se trató, pues, de un transporte interespecie, desde la luz hacia la materia.

En resumen: los avances realizados en el campo de la teleportación cuántica son imparables y se suceden continuamente, abarcando fotones y partículas materiales, así como variados tipos de propiedades. Junto a todos estos logros, se está produciendo un desarrollo paralelo de las técnicas de corrección de errores en las transmisiones cuánticas. Para ello se requieren nuevos procedimientos no clásicos, ya que, por ejemplo, la redundancia, el enviar repetidos pulsos con la misma información, no es posible, al estar proscritas las duplicaciones de los estados cuánticos. A estas alturas nadie se sorprenderá si decimos que casi todas esas técnicas recurren al entrelazamiento cuántico, recurriendo a codificar cada bit cuántico en estados entrelazados de varios qubits, más robustos frente a la decoherencia que los de un solo qubit. Estos estados se transmiten y luego se procede a su descodificación; puesto que contienen información adicional a la que se quiere transmitir, pueden corregirse posibles errores producidos en el proceso. Ejemplos de estos procedimientos, que configuran por sí solos una nueva disciplina en la teoría cuántica de la información, la QEC (*Quantum Error Correction*, corrección de errores cuánticos), son los protocolos pioneros de corrección de errores propuestos en 1996 por Peter Shor y Robert Calderbank, por un lado, y Andrew Steane, por otro, que hacían uso de estados de 9 y 7 qubits, respectivamente. La QEC incluye tanto técnicas pasivas —corrección de errores producidos— como activas —prevención y supresión de errores—; como meta primordial, se pretende conseguir implementar canales cuánticos de comunicación tolerantes a cierta tasa de errores, los inevitables *ruidos* omnipresentes en toda transmisión y en todo dispositivo como, por ejemplo, un computador cuántico. También se incorporan técnicas de *destilación de entrelazamiento*, que eliminan el ruido o las alteraciones que puedan producirse en el par entrelazado, algo usual y que hay que controlar en un proceso de teleportación.

> El sueño de la teleportación es ser capaz de viajar mediante la simple reaparición en un lugar distante.
>
> DIRK BOUWMEESTER

TELEPORTANDO... ¿PARA QUÉ?

Como hemos visto, teleportar es hoy algo realizable y realizado de muchas formas, bien entendido que el correspondiente fenómeno cuántico no tiene nada que ver con lo que se representa bajo esa denominación en la mayoría de las obras de ciencia ficción (maravillosas series como *Star Trek* y demás). La pregunta inmediata es: además de la belleza intrínseca y lo sugestivo del fenómeno, ¿para qué nos puede ser útil?

Las principales aplicaciones en las que sin duda el fenómeno de la teleportación va a intervenir en el futuro son el desarrollo de redes cuánticas para la distribución de información y, cómo no, la construcción de los anhelados computadores cuánticos. Hemos dicho que la información se almacena en qubits, pero el problema de los estados entrelazados es que son muy

inestables, se desploman fácilmente a la menor interacción, y es muy difícil prevenir la acción del entorno sobre los sistemas cuánticos, la llamada decoherencia, cuando se pretende que esa información recorra largas distancias o permanezca almacenada durante tiempos largos. Con la teleportación, se abre una nueva vía para contrarrestar este problema y hacer posible el intercambio de qubits entre lugares lejanos: los qubits se pueden transferir a distancia sin que tengan que recorrer el camino intermedio.

De modo que la teleportación cuántica se ha configurado como una herramienta muy útil, en definitiva, tanto para el futuro de la computación cuántica como para el desarrollo de redes cuánticas de comunicación, abiertas o con seguridad y cifrado basados en protocolos cuánticos (la criptografía cuántica, con procesos de distribución segura de claves ya desarrollados e incluso comercializados).

¿Se podría llegar a teleportar un animal?

Hemos visto que la teleportación lo es de información: reproducimos información condensada en qubits, trasladada desde un sistema hacia otro que ocupa un lugar que va consiguiéndose que sea cada vez más distante. Se replica el estado original del primer sistema sobre el segundo (el estado cuántico, ya que el sistema receptor puede ser de distinta naturaleza al original); el estado del sistema donante de estado queda alterado (no hay duplicación cuántica de estados) y se requiere el concurso de un canal clásico de transferencia de información (no hay transmisión instantánea de información: no hay conflicto con la relatividad).

Hay una pregunta quizá perturbadora que surge ante el fenómeno cuántico de la teleportación: ¿la identidad o mismidad de un sistema se la confieren la materia o luz que lo componen —sus átomos y fotones específicos integrantes— o solo el estado cuántico que lo describe? Dicho en otras palabras, si lográramos en un lejano futuro teleportar el estado cuántico global de

todos, absolutamente todos, los elementos (moléculas, átomos, electrones, fotones, quarks...) que constituyen una oveja dada, llamémosla Dolly, proceso en que la dejaríamos completamente alterada (óbito probable), sobre un conjunto de elementos componentes idénticos situados en otro lugar distante, ¿el nuevo sistema sería Dolly? Desde luego luciría igual, y recordaría y sentiría igual, dicho sea con permiso de algunos neurocientíficos, dejando al margen la evanescente alma y suponiendo que el estado cuántico es la última y más completa descripción posible para un sistema.

> No, jamás olvidaré aquel cráneo aplastado, aquella cabeza de pesadilla, blanca, velluda, con puntiagudas orejas de gato y ojos protegidos por grandes placas oscuras.
>
> GEORGE LANGELAAN, *LA MOSCA*

Además, hay algo muy inquietante, un peligro que acecha y que convirtió al protagonista del relato *La mosca*, de George Langelaan, en un monstruo: a la mínima intrusión de una interacción perturbadora en el proceso, ¿qué nuevo ser se habría fabricado? La decoherencia, simplemente, podría actuar como una diosa terrible, creadora y aniquiladora.

Desde luego, no es que se atisbe semejante logro en el horizonte: hay estimaciones que indican que para teleportar un objeto de unos pocos gramos habría que teleportar en torno a 10^{30} bits de datos; se calcula que hay alrededor de 10^{29} partículas materiales en un cuerpo humano, con variados tipos de propiedades cada una... ¿Qué medios se requerirían? ¿Cuánto tiempo llevaría? Aunque quizá bastaría teleportar el cerebro, el resto podría duplicarse clásicamente. En todo caso, hoy por hoy (y por siglos... o billones de años) ni siquiera resulta imaginable, es implanteable y queda descartado por completo. Pero ¿se trata solo de una limitación de medios? ¿No hay una limitación fundamental, de principios o leyes? ¿Tal vez sí de principios morales? Y si el «donante» no muere, sino que pervive convertido en otro ser, con su identidad irremediablemente alterada, ¿serían dos seres distintos, sin más conexión que haber estado en el mismo estado cuántico, en dos instantes diferentes de su existencia? Y ya puestos, en una teleportación interespecies, ¿no podría te-

leportarse un ser humano sobre un material menos fungible que la *carne*? ¿Quizá sobre un ordenador cuántico? ¿El ente destino podría ser considerado legalmente el reemplazo en sociedad del donante original? Transhumanismo, cíborgs... *Star Trek*, al lado de todo esto, es un juego de niños.

CAPÍTULO 3

Computación cuántica

No sabemos si el ser humano nació primero y después creó los números, o si ya estaban ahí y solo los descubrió... Pero sí sabemos que no podemos parar de contar y de calcular. Las computadoras son imprescindibles para la ciencia, y también para la vida contemporánea, al menos en nuestra desarrollada parte del mundo. Y las queremos cada vez más potentes.

Nuevos tiempos, nuevas máquinas. Siempre ha sido así, y en estos acelerados años contemporáneos es difícil prever qué nuevas sorpresas tecnológicas, ideadas en un pasado no muy lejano como sueños quiméricos, irrumpirán de pronto en nuestra cotidianidad. ¿Estarán entre ellas los ordenadores cuánticos, cuando todavía muchos bregan por entenderse con los clásicos? No está claro si los consumidores domésticos acabarán navegando por las webs de un internet cuántico en computadores también cuánticos, pero lo que sí puede afirmarse hoy en día es que la computación cuántica, entendida en el sentido de disponer de un dispositivo que funcione basándose en entes que ocupan estados superpuestos y entrelazados, ha dejado de ser una quimera. Aunque estemos, eso sí, en sus inicios.

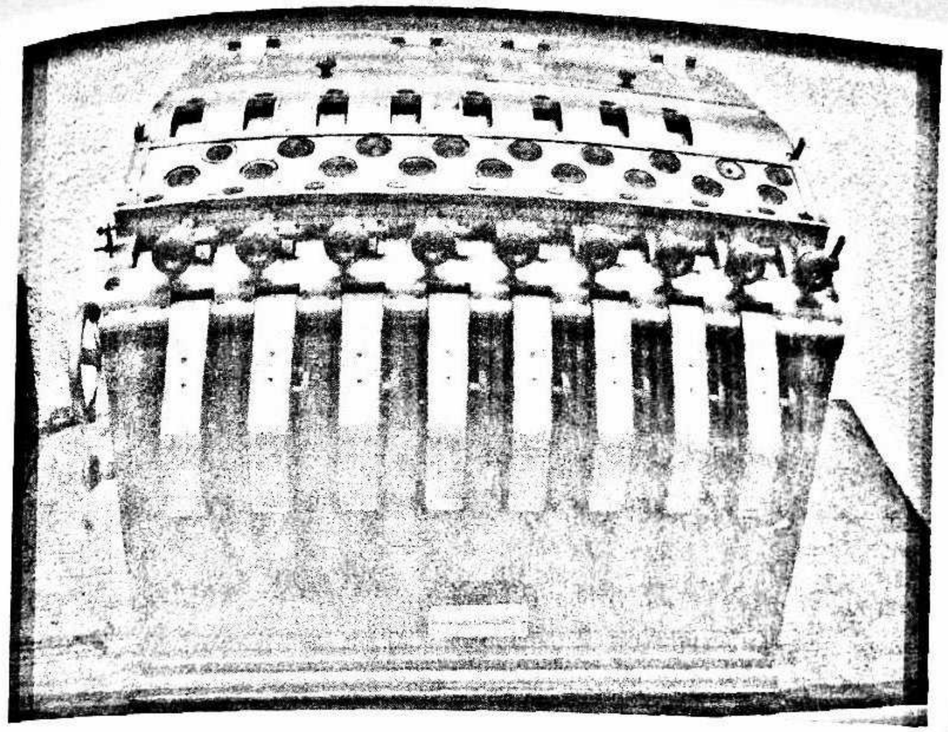
EN EL PRINCIPIO FUE EL ÁBACO, Y DESPUÉS LLEGARON LOS ORDENADORES PORTÁTILES

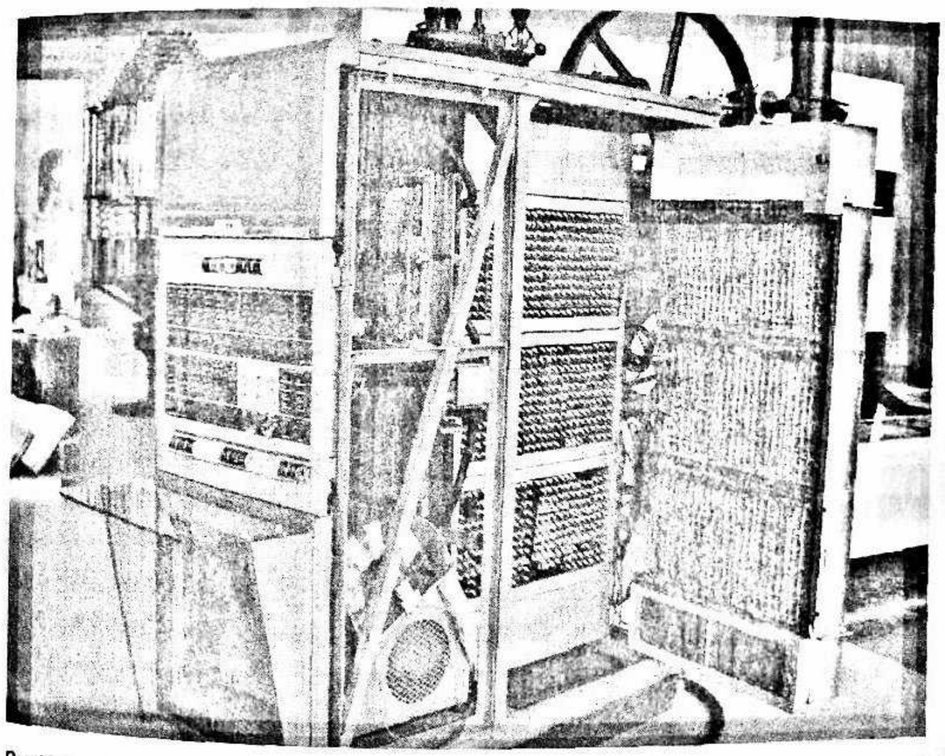
Cuando los cálculos matemáticos se van complicando, la humanidad diseña instrumentos que ayudan a manejar los números y

sus operaciones, y desde los antiguos ábacos hasta los ordenadores actuales, la computación se ha convertido en una herramienta indispensable para el progreso. En el siglo xx, entre otros muchos nombres decisivos para la consolidación científica de la computación, queremos destacar tres: Alan Turing, que concibió en 1937 la denominada «máquina universal de computación», constructo ideal capaz de ejecutar todas las operaciones matemáticas de cualquier algoritmo mediante sucesivos pasos mecánicos, según la indemostrada pero imbatida tesis de Church-Turing; John von Neumann, diseñador de la arquitectura para un computador digital electrónico general en 1945 y creador de nuevos y potentes algoritmos, y, en tercer lugar, la empresa IBM *(International Business Machines)*, cuyo computador IBM650, que puede verse en la fotografía inferior de la página contigua, fue el primero que se fabricó a gran escala, vendiéndose unas 2 000 unidades entre 1954 y 1962.

> Es indigno de hombres excelentes desperdiciar las horas como esclavos en la labor de calcular lo que sin riesgo podría relegarse a alguien más si se utilizaran máquinas.
>
> **Gotfried Leibniz**

Podemos definir una computadora, de manera muy general, como una máquina que almacena y procesa información, generando una respuesta en forma de un conjunto de datos en correspondencia con otro conjunto de datos de entrada; la adecuación de la respuesta viene regida por un programa que determina las operaciones de procesamiento. Si las primeras computadoras tenían un interior analógico, que trabajaba con variaciones continuas de oscilaciones de voltaje y frecuencia, posteriormente se transformaron en digitales, lo que las hizo aptas para manejar variados programas *(software)* sin tener que modificar su composición interna o de circuitería *(hardware)*. De modo que, tras las iniciales electroválvulas de las computadoras analógicas, llegaron los transistores, y luego los circuitos integrados. Cuando se incorporaron los microprocesadores, circuitos integrados de alta densidad, las computadoras digitales se vendieron a millones y la informática inundó nuestros hogares.





Dos hitos en la historia de la computación. Arriba, el aritmómetro electromecánico de 1920 de Leonardo Torres Quevedo, la primera calculadora digital de la historia, hoy en el museo de Madrid a él dedicado. Abajo, la computadora IBM650, el primer ordenador fabricado a gran escala.

COMPUTACIÓN CLÁSICA: PUERTAS PARA UN ÁLGEBRA BOOLEANA

La computación, en definitiva, concierne a la información: cómo se adquiere, se representa, se procesa, se almacena, se transmite, se transforma. La información en una computadora moderna —clásica— se codifica en bits, las unidades mínimas de almacenamiento de información, definidos como variables dicotómicas, es decir, que solo pueden tomar dos valores, usualmente representados como bit 0 y bit 1, por convención, valor falso (F o 0) y valor verdadero (V o 1). Físicamente, se implementan como diferentes niveles de voltaje en un dispositivo semiconductor, de forma que en computación se sustituye el sistema decimal de numeración por el binario, en el que recordemos que un número x se expresa mediante sus «componentes» o bits (n_{N-1}, n_{N-2},..., n_2, n_1, n_0), donde cada n_i es 0 o 1, teniéndose:

$$x = n_{N-1}\cdot 2^{N-1} + n_{N-2}\cdot 2^{N-2} + \ldots + n_2\cdot 2^2 + n_1\cdot 2^1 + n_0\cdot 2^0,$$

donde n_{N-1} se define como el bit «más significativo», mientras que n_0 establece el «menos significativo». De esta forma, los primeros diez números (0, 1, 2,..., 9) se codificarían en un sistema binario posicional de cuatro bits como:

0	1	2	3	4	5	6	7	8	9
0000	0001	0010	0011	0100	0101	0110	0111	1000	1001

Por ejemplo, $7 = 0\cdot 2^3 + 1\cdot 2^2 + 1\cdot 2^1 + 1\cdot 2^0$, de modo que este sistema de cuatro bits permitiría codificar los números entre el 0 (0000) y el $2^4 - 1 = 15$ (1111). Para codificar los números naturales entre 0 y 255, se necesitarán como mínimo ocho bits (un *byte*), ya que $2^8 = 256$. En general, el empleo de N bits (N posiciones) permite codificar los números naturales entre 0 y $2^N - 1$.

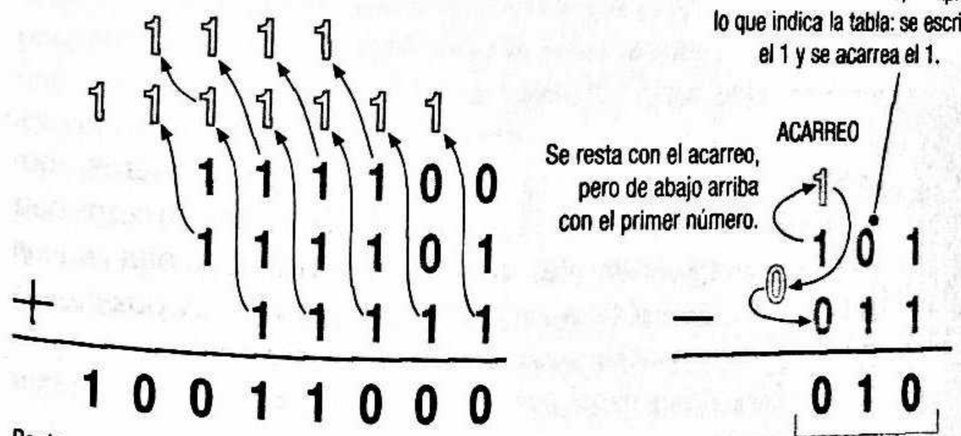
Para procesar la información, las computadoras aplican el *álgebra booleana*, desarrollada en el siglo XIX por el matemático George Boole para manejar expresiones de la lógica proposicional, en la que los enunciados (como, por ejemplo, «Ahora está

APRENDIENDO DE NUEVO A SUMAR Y RESTAR... EN BINARIO

Estamos acostumbrados a manejar el sistema decimal en las operaciones matemáticas cotidianas, pero también el sistema binario, por ejemplo, cada vez que manejamos un ordenador. Este sistema es de base dos: opera con solo dos caracteres (el sistema decimal o en base diez emplea diez), llamados *bits* (contracción de *binary digits*). Para sumar o restar dos números binarios, se empieza sumando o restando los bits menos significativos, produciendo bits de suma y bits de acarreo. Se continúa operando con los sucesivos bits de derecha a izquierda, incorporando en su caso el acarreo, según las reglas de la tabla de suma en la figura. La resta binaria se realiza de manera similar, pero empleando acarreos negativos o «préstamos» a una columna desde la columna anterior cuando el minuendo de esa columna sea un 0, y el sustraendo, un 1. Así, para restar dos números binarios se restan primero los bits menos significativos, produciendo bits de resta y bits de préstamo. Se continúa procesando bits de derecha a izquierda, restando cada bit de préstamo, si lo hubiera, de la siguiente columna a la izquierda, de modo que cada vez que hay un préstamo, la correspondiente posición del minuendo que presta pasa de 1 a 0; si ya era 0, pasa a 1, y se tomaría de la siguiente posición, que pasaría a ser 0 si fuera 1 (si fuera 0, se pone a 1 y se pediría a la siguiente, y así hasta que se tope con un 1).

SUMA	RESULTADO	ACARREO
0+0	0	
0+1	1	
1+0	1	
1+1	0	1 a la siguiente columna

RESTA	RESULTADO	PRÉSTAMO
0−0	0	
0−1	1	1 de la siguiente columna
1−0	1	
1−1	0	



Reglas para sumar y restar en binario y un ejemplo de cada operación.

lloviendo aquí») se conciben como variables, con valor verdadero (V) o falso (F), y se representan por letras del alfabeto. Las relaciones y operaciones entre las variables se representan por símbolos especiales, como $\vee$ (disyunción no exclusiva), $\wedge$ (conjunción) y ' (negación). Estos operadores o funciones relacionan las proposiciones, y el *valor de verdad* resultante se establece mediante unas *tablas de verdad*, que se muestran en la figura 1, con la convención $V \equiv 1$ y $F \equiv 0$ (donde el símbolo $\equiv$ significa «idéntico»). Por ejemplo, para la conjunción de dos enunciados A y B, es decir, la proposición $C = A \wedge B$, se tiene que C solo es verdadera cuando lo son A y B; en otro caso, C es falsa. Y en la operación negación de un enunciado dado A, simbolizado por la proposición $C = A'$, se invierte su valor de verdad, de modo que C es verdadera cuando A es falsa, y viceversa.

Las operaciones o procesos básicos a los que se somete de forma primaria la información en un computador se corresponden con las denominadas *puertas lógicas*, unos dispositivos electrónicos generales que implementan las operaciones lógicas básicas sobre los bits y que proporcionan otro modelo abstracto de concebir todo ordenador, adicional al modelo de Turing. En correspondencia con un álgebra de Boole se pueden definir operaciones unarias, que solo necesitan un bit para producir un resultado, como la negación (función NOT), y operaciones binarias, que requieren de dos, como la conjunción (función AND, correspondiente al operador $\wedge$), la disyunción no exclusiva (función OR, correspondiente al operador $\vee$) y la disyunción exclusiva XOR (que varía respecto a la OR en que la disyunción entre dos proposiciones verdaderas es falsa; compárense las correspondientes tablas de verdad en la figura 1). En electrónica, es convencional representar los correspondientes circuitos simples que se corresponden con las distintas puertas lógicas como se indica en la figura 1, donde se proporcionan los símbolos para algunas puertas lógicas clásicas, así como las tablas de verdad de los operadores lógicos asociados.

Como veremos a continuación, el desarrollo de una computación cuántica general conservará el concepto de puertas lógicas, pero las implementará con modificaciones profundas.

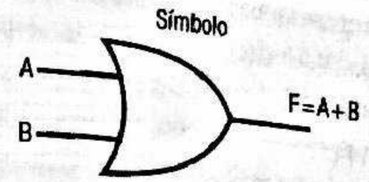
FIG. 1

FUNCIÓN OR, PUERTA OR

Tabla de verdad

A	B	A+B
0	0	0
0	1	1
1	0	1
1	1	1

Símbolo

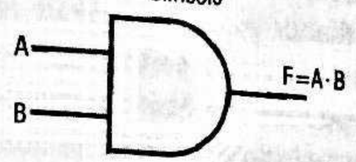


FUNCIÓN AND, PUERTA AND

Tabla de verdad

A	B	A·B
0	0	0
0	1	0
1	0	0
1	1	1

Símbolo



FUNCIÓN NOT, INVERSOR

Tabla de verdad

A	A'
0	1
1	0

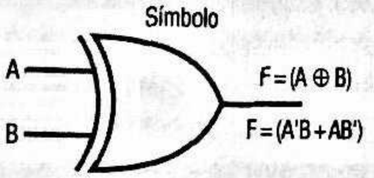
Símbolo

FUNCIÓN XOR, PUERTA XOR

Tabla de verdad

A	B	A⊕B
0	0	0
0	1	1
1	0	1
1	1	0

Símbolo



Algunas puertas o procesos básicos en teoría clásica de la información y sus tablas de verdad asociadas ($1 \equiv V$ y $0 \equiv F$). Para representar las funciones OR, XOR, AND y NOT suelen emplearse los símbolos +, $\oplus$, $\cdot$ y ', respectivamente. Un conjunto de puertas integra un sistema completo cuando todas las operaciones expresables en matemática binaria pueden reducirse a ellas, es decir, permiten implementar cualquier función lógica estándar. Por ejemplo, son conjuntos completos: {OR, AND, NOT}, {AND, NOT}, {OR, NOT}.

COMPUTACIÓN CUÁNTICA: OPERANDO EN PARALELO SOBRE QUBITS

El futuro de los ordenadores clásicos, en el progreso hacia la miniaturización, también es cuántico. Pero con el nombre de «computación cuántica» no nos referimos en general a ese futuro, sino a la construcción de una máquina de computación que opere de forma cuántica, es decir, que almacene y procese la información no en forma de bits, sino de qubits, que funcione manteniendo en su interior entes que ocupen estados cuánticos de superposición y con entrelazamiento y se conserven en dichos estados.

Podemos concebir que todo cálculo que pueda implementarse mediante puertas lógicas clásicas deberá poder realizarse mediante puertas cuánticas, es decir, que cualquier algoritmo clásico podrá ser implementado sobre un ordenador cuántico. Pero, y he aquí el interés, la idea es que las características puramente cuánticas, específicamente la superposición y el entrelazamiento, proporcionen una mayor eficacia al abordar determinado tipo de problemas, por ejemplo, en algo tan crucial para la economía de nuestro mundo moderno como la factorización de números grandes (un problema matemático del cual, como veremos al abordar la criptografía, depende hoy en día la seguridad en las comunicaciones). Para ello se necesitan programas y algoritmos cuánticos, que sepan aprovechar las leyes cuánticas y que se puedan ejecutar sobre máquinas cuánticas. Pero, hoy por hoy, tan solo se dispone de apenas unos pocos de ellos y, además, todavía no existen máquinas cuánticas con la suficiente potencia como para aplicarlos sobre problemas que involucren un gran número de datos. Y es que, como vamos a ver, se afrontan nuevos y enormes problemas al construir un ordenador cuántico. Uno muy importante es la necesidad de lograr un eficaz escalamiento, es decir, conseguir un diseño que, conservándose en su concepción esencial, permita ir ampliando la potencia de cálculo, desde el manejo de un pequeño número de qubits hacia un número cada vez mayor de ellos. De modo que, más allá de meritorios prototipos, puede decirse que no existe todavía una «industria» de la computación cuántica totalmente desarrollada.

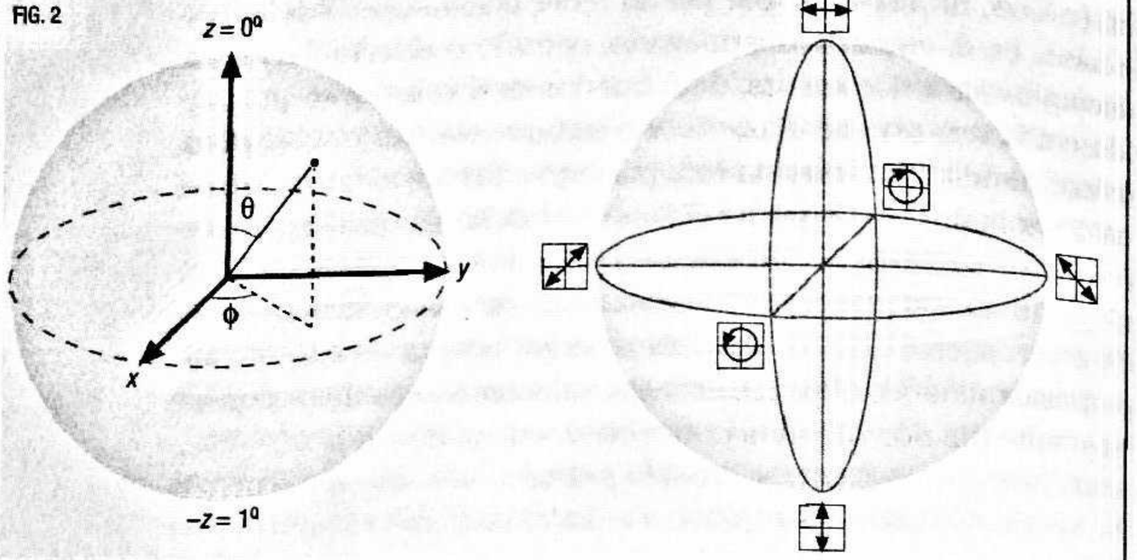
Sabemos que la pieza básica de la información clásica es el bit (o Cbit, bit clásico), que puede tener dos valores: verdadero o falso, 1 o 0, encendido o apagado, cerrado o abierto. La lógica clásica establece como axioma que los dos valores no pueden darse a la vez: o se tiene un valor o se tiene el otro, y la máquina universal de Turing respeta este principio. Frente al bit, en teoría cuántica la unidad de información es el qubit (o Qbit) que, conforme a su cuántica naturaleza, aunque también dicotómico en su rango de valores posibles como resultado de una medida (o falso, 0^q, o verdadero, 1^q), puede, sin embargo, ocupar estados de superposición de los estados correspondientes a esos dos valores:

$$\psi = a \cdot 0^q + b \cdot 1^q,$$

donde 0^q y 1^q son los dos qubits básicos, implementables físicamente mediante un par de estados cuánticos fundamentales. El hecho de que el qubit sea una superposición de dos estados fundamentales no significa que al leer la información codificada sobre él se pueda extraer una cantidad infinita de ella, como parecería corresponderse con el hecho de que los pares diferentes de valores posibles para a y b son infinitos. Al efectuar una medida sobre un qubit, el registro de lectura informa solo de una de las dos posibilidades, 0^q o 1^q, nunca de una superposición, conforme al postulado cuántico del colapso de la función de onda. Un qubit puede representarse mediante la denominada *esfera de Bloch*, de radio unidad, que permite asociar cada punto sobre su superficie con cada estado posible del qubit, según se representa en la figura 2.

La información que encierra un qubit puede implementarse físicamente de variadas maneras. Cuando se recurre a la polarización de un fotón, escogiendo un par cualquiera de estados fundamentales, como $\rightarrow$ y $\uparrow$, el resultado es un qubit fotónico. Solo hay que convenir en que la polarización horizontal va a constituir el qubit fundamental 0^q, y la perpendicular o vertical, su compañero 1^q (o al revés). También se puede implementar un qubit material, recurriendo a electrones, o átomos de espín 1/2, y escogiendo un par de estados fundamentales de tercera componente de espín, estados «hacia arriba» y «hacia abajo», conviniendo en tomar,

FIG. 2



Esfera de Bloch o representación geométrica espacial de los posibles estados de un qubit general. Se establece una correspondencia entre cada punto sobre la superficie de una esfera de radio unidad y un estado particular del qubit general, $\psi = a\cdot 0^{Q} + b\cdot 1^{Q}$, con $|a|^2+|b|^2=1$; los dos polos se asocian con los estados básicos 0^{Q} y 1^{Q}. A la izquierda, representación general; a la derecha, aplicación al caso particular de representación para un qubit implementado en términos de los estados de polarización fotónicos: con la convención hecha en el texto, los polos norte y sur de la esfera se corresponden con las polarizaciones horizontal y vertical, respectivamente. Se indican también los puntos asociados a las dos polarizaciones diagonales y a las dos polarizaciones circulares, dextrógira y levógira. Los restantes puntos sobre la superficie esférica corresponderían a estados de polarización elíptica.

por ejemplo, el estado de espín hacia arriba para 0^{Q} y el estado hacia abajo para 1^{Q}. Otra implementación muy usada, sobre todo con trampas de iones, es recurrir a dos estados posibles de energía, E_1 (0^{Q}) y E_2 (1^{Q}), de un sistema cuántico, como un ion atómico. En cualquier caso, la superposición de estados:

$$\psi = a\cdot 0^{Q} + b\cdot 1^{Q}, \text{ con } |a|^2+|b|^2=1$$

constituirá una implementación cabal de un qubit general, lo que vamos a denominar un 1-qubit.

Si disponemos de dos qubits (dos 1-qubits, cada uno implementado sobre un sistema de un elemento: un fotón, un electrón, un ion, etc.), el nuevo espacio global de estados cuánticos corresponderá al denominado en matemáticas *producto tensorial* de los estados de cada qubit, que aquí simplemente vamos a representar por el símbolo ×, y que ya usamos para multiplicar funciones de onda de distintas partículas en el capítulo 1. Por ejemplo, para dos qubits, 1 y 2, tenemos que un posible estado conjunto (no entrelazado) sería el producto directo de los correspondientes dos estados asociados a cada qubit, que según vimos también en el primer capítulo tiene la expresión:

$$\Psi(1,2) = \Psi(1)\times\Psi(2) = (a_1\cdot 0^{Q}{}_1 + b_1\cdot 1^{Q}{}_1)\times(a_2\cdot 0^{Q}{}_2 + b_2\cdot 1^{Q}{}_2).$$

Desarrollando todos los productos y sumas, es fácil llegar a la siguiente función de onda para el sistema de dos qubits:

$$\Psi(1,2) = \Psi(1)\times\Psi(2) =$$
$$= (a_1\cdot a_2)\cdot(0^{Q}{}_1\times 0^{Q}{}_2) + (a_1\cdot b_2)\cdot(0^{Q}{}_1\times 1^{Q}{}_2) +$$
$$+ (b_1\cdot a_2)\cdot(1^{Q}{}_1\times 0^{Q}{}_2) + (b_1\cdot b_2)\cdot(1^{Q}{}_1\times 1^{Q}{}_2).$$

Obviando los índices de partícula y los símbolos de producto tensorial, este estado se suele escribir abreviadamente como:

$$\Psi(1,2) = \Psi(1)\times\Psi(2) =$$
$$= \alpha_0\cdot(0^{Q}\times 0^{Q}) + \alpha_1\cdot(0^{Q}\times 1^{Q}) + \alpha_2\cdot(1^{Q}\times 0^{Q}) + \alpha_3\cdot(1^{Q}\times 1^{Q}) \equiv$$
$$\equiv \alpha_0\cdot(00)^{(2Q)} + \alpha_1\cdot(01)^{(2Q)} + \alpha_2(10)^{(2Q)} + \alpha_3\cdot(11)^{(2Q)}$$

donde α_0, α_1, α_2 y α_3 simbolizan cuatro números (complejos, en general). Esta expresión representa un 2-qubit, un estado para dos qubits (dos 1-qubits), y lo hace como una suma o combinación de cuatro estados fundamentales del sistema de dos qubits, los cuatro estados $\{(00)^{(2Q)}, (01)^{(2Q)}, (10)^{(2Q)}, (11)^{(2Q)}\}$. De modo que, si para un 1-qubit teníamos pares de estados fundamentales, para un sistema de 2-qubit (dos 1-qubits) tenemos cuartetos: el número se ha doblado (en computación, cada uno de estos conjuntos de estados fundamentales se suele denominar *base computacional*). En consecuencia, también se han doblado los números que especifican cada estado: si antes nos bastaba una pareja (a, b), cuyos módulos al cuadrado debían sumar la unidad ($|a|^2+|b|^2=1$), ahora aparecen cuatro (α_0, α_1, α_2 y α_3), que deben

satisfacer, análogamente, que la suma de los cuadrados de sus módulos sea igual a la unidad. Si comparamos con el caso clásico, para especificar el estado de dos bits necesitamos solo dos números reales; en el caso cuántico, para dos 1-qubits se requieren cuatro números complejos.

Todo estado posible de un sistema de dos qubits, entrelazado o no, puede expresarse, a partir de cuatro constantes (α_0, α_1, α_2 y α_3), como una suma o combinación de las funciones del anterior cuarteto fundamental, constituido por estados no entrelazados. De hecho, la mayoría de las elecciones para los valores de las cuatro constantes α conducirán a un estado entrelazado, es decir, no factorizable como producto de dos estados individuales de los dos qubits. Un ejemplo claro son los cuatro estados de Bell, que constituyen una base computacional alternativa para el sistema de dos qubits. En términos de la esfera de Bloch, corresponden a una superposición en que ninguno de los dos qubits tiene asociada una posición determinada sobre ella.

Para almacenar una información dada requeriremos un gran número de qubits, pudiendo asociar cada uno de ellos con un registro de información. En general, para representar un estado de N qubits se precisará una base computacional (conjunto de estados fundamentales) de 2^N elementos. Si comparamos con los N valores reales que se necesitan para especificar información en N bits clásicos, vemos que, mientras que con N bits se codifican 2^N datos, con N qubits las posibilidades se amplían vertiginosamente, al poder superponer los 2^N estados de la base. Se denomina *paralelismo cuántico* esa gran capacidad adicional que proporcionan las superposiciones cuánticas para almacenar información y procesarla de forma simultánea. Pero hay que tener presente que, para explotarlo, harán falta buenos algoritmos, que consigan que, al leer la información almacenada, el colapso cuántico de la superposición conduzca a la solución óptima al problema planteado, y no a otra (más adelante ilustraremos esta situación). Y no es fácil desarrollarlos.

Si se disponen de N qubits, la expresión general para una serie de N registros de 1-qubit no entrelazados, extensión directa de la anterior para el 2-qubit, sería el N-qubit:

$$\Psi(1, 2, \ldots, N) = \psi(1) \times \psi(2) \times \ldots \times \psi(N),$$

estando la base computacional del espacio matemático para los N qubits integrada por los 2^N estados fundamentales:

$$(000 \ldots 00)^{(NQ)} \equiv (0^Q{}_1) \times (0^Q{}_2) \times (0^Q{}_3) \times \ldots \times (0^Q{}_{N-1}) \times (0^Q{}_N)$$
$$(000 \ldots 01)^{(NQ)} \equiv (0^Q{}_1) \times (0^Q{}_2) \times (0^Q{}_3) \times \ldots \times (0^Q{}_{N-1}) \times (1^Q{}_N)$$
$$\ldots$$
$$(100 \ldots 10)^{(NQ)} \equiv (1^Q{}_1) \times (0^Q{}_2) \times (0^Q{}_3) \times \ldots \times (1^Q{}_{N-1}) \times (0^Q{}_N)$$
$$\ldots$$
$$(111 \ldots 11)^{(NQ)} \equiv (1^Q{}_1) \times (1^Q{}_2) \times (1^Q{}_3) \times \ldots \times (1^Q{}_{N-1}) \times (1^Q{}_N)$$

donde en cada línea hay presentes N factores.

Cualquier estado del espacio asociado a los N qubits, entrelazado o no, se puede expresar como una superposición de estos 2^N estados o N-qubits fundamentales, mediante su adecuada combinación o suma, multiplicados por los números complejos α adecuados. Así pues, cada N-qubit fundamental en particular posee la expresión general $(n_{N-1}, n_{N-2}, \ldots, n_2, n_1, n_0)^{(NQ)}$, esto es, en esencia, una hilera de N números de valor 0 o 1. Los 2^N estados se pueden numerar, por tanto, sin más que hacer corresponder cada uno con el número decimal que expresa en binario, según la conocida descomposición $x = n_{N-1} \cdot 2^{N-1} + n_{N-2} \cdot 2^{N-2} + \ldots + n_2 \cdot 2^2 + n_1 \cdot 2^1 + n_0 \cdot 2^0$, en un rango que abarca desde $x = 0$ —el estado $(000\ldots00)^{(NQ)}$— hasta $x = 2^N - 1$ —el estado $(111\ldots11)^{(NQ)}$—. Esta nueva forma de denominar y numerar los estados de la base computacional se denomina decimal. Por ejemplo: para un qubit, los dos estados fundamentales $\{0^Q, 1^Q\}$ serían, respectivamente, el $0^{(1Q)}$ y el $1^{(1Q)}$ en notación decimal; para un 2-qubit, el cuarteto fundamental se numeraría:

$$\{(00)^{(2Q)} = 0 \cdot 2^1 + 0 \cdot 2^0 \equiv 0^{(2Q)}, (01)^{(2Q)} =$$
$$= 0 \cdot 2^1 + 1 \cdot 2^0 \equiv 1^{(2Q)}, (10)^{(2Q)} \equiv 2^{(2Q)}, (11)^{(2Q)} \equiv 3^{(2Q)}\}.$$

Veamos ahora algunos ejemplos de paralelismo cuántico. El primero ya está dado: mientras que un bit clásico solamente pue-

de tomar uno de los dos valores discretos, 0 o 1 (digamos que solo puede situarse sobre uno de los dos polos de la esfera de Bloch), un qubit representa de forma continua y a la vez todos los valores superpuestos $a \cdot 0^{Q} + b \cdot 1^{Q}$. Como segundo ejemplo, consideremos un número natural entre 0 y 7, que para ser almacenado sobre bits clásicos requiere del uso de al menos tres bits. Pero si disponemos de tres registros cuánticos, tres 1-qubits, es decir, un 3-qubit, a partir del octeto fundamental, integrado por los ocho 3-qubits fundamentales:

$$\{(000)^{(3Q)} \equiv 0^{(3Q)}, (001)^{(3Q)} \equiv 1^{(3Q)}, (010)^{(3Q)} \equiv 2^{(3Q)}, ..., (111)^{(3Q)} \equiv 7^{(3Q)}\}$$

el 3-qubit general superposición de ellos:

$$\Psi(1, 2, 3) = \alpha_0 \cdot (000)^{(3Q)} + \alpha_1 \cdot (001)^{(3Q)} + \ldots + \alpha_7 \cdot (111)^{(3Q)},$$
$$\equiv \alpha_0 \cdot (0)^{(3Q)} + \alpha_1 \cdot (1)^{(3Q)} + \ldots + \alpha_7 \cdot (7)^{(3Q)}$$

nos permitirá codificar no solo cualquier número entre el 0 y el 7, como en el caso clásico, sino también, sobre los tres registros cuánticos, muchísima más información, condensada en el estado superposición cuántica (a partir de los distintos conjuntos de valores de las ocho constantes $\alpha_0, \alpha_1, ..., \alpha_7$). Y, además, será posible realizar cálculos de forma paralela, por ejemplo, operar calculando simultáneamente los ocho valores $F[x^{(3Q)}]$ de una función $F[x]$ dada.

Así pues, y para hacernos una idea de la importancia del paralelismo cuántico, si tenemos N bits clásicos seremos capaces de almacenar la información correspondiente a un solo número entero de entre 2^N posibles; si tenemos N qubits, como podemos formar superposiciones de los 2^N estados de la base computacional, cada una especificada por un conjunto de 2^N números complejos (los números α), la capacidad de la memoria disponible se incrementa enormemente. Además, surge la posibilidad de procesar información en paralelo de forma masiva: por ejemplo, podremos evaluar una función $F(x)$ simultáneamente para múltiples 2^N valores de su argumento, x, en una sola operación, almacenando así una cantidad ingente de registros clásicos en un solo estado cuántico. Pero hay que tener siempre presente que, puesto que la medida o lectura de esa superposición la colapsará, proporcionando finalmente y de forma probabilística solo uno de los posibles resultados antes superpuestos, se necesitarán procedimientos para garantizar que la información específica que se busca sea la que aflore al final. Para ello, se pueden forzar las interferencias adecuadas para conseguir suprimir, o hacer menos probables, los estados en la superposición que no contengan la información útil para resolver cada problema, mientras que se aumenta, por medio de las pertinentes interferencias constructivas, la probabilidad de que las medidas finales colapsen los estados hacia los que proporcionen la información buscada. En un ejemplo desarrollado por Jesse Dunietz, es como si buscáramos una llave de hierro (la solución óptima de un problema) entre un montón de miles de aluminio (la superposición que constituye el paralelismo); en cada oportunidad solo podemos coger una y perdemos el acceso a las otras (al medir, la superposición colapsa al azar a una sola de todas las funciones superpuestas y desaparecen las demás). Si queremos encontrar rápidamente la llave, tenemos que idear algo que podamos hacer sobre todas las llaves, sin romperlas (sin desplomar la superposición), y que aumente la probabilidad de que saquemos la buena. Por ejemplo, pasar un imán por encima del montón de llaves, que hará que la de hierro se mueva hacia él, destacándose de entre las restantes. Eso es lo que deberá hacer un algoritmo cuántico eficaz.

Puertas lógicas cuánticas

En computación cuántica general, las operaciones sobre los qubits se realizan mediante puertas lógicas también cuánticas, algunas de las cuales serán generalizaciones de las clásicas y otras, por el contrario, surgirán como novedad. Un primer hecho sobre las puertas lógicas cuánticas que cabe destacar es que, a diferencia de lo que ocurre para las clásicas, todas son reversibles. Para entender qué significa esto, imaginemos que una puerta lógica es

un dispositivo general que proporciona una salida a partir de una entrada; pues bien, cuando la salida permite reconstruir la entrada, se dice que la puerta es reversible. Por ejemplo, la puerta lógica clásica NOT es claramente reversible: actuando sobre un 0 escribe un 1, y viceversa, luego basta con colocar dos puertas NOT seguidas para conseguir la reversibilidad. En cambio, una puerta como, por ejemplo, la clásica AND, es irreversible: puesto que se tiene una sola salida a partir de dos entradas, hay tres posibles situaciones que pueden conducir a una misma salida 0 (las tres entradas 00, 01 y 10 conducen a ella, según se desprende de la correspondiente tabla de verdad en la figura 1, pág. 83), siendo, en consecuencia, imposible revertirla. El problema asociado a las puertas lógicas irreversibles es que sus implementaciones físicas necesariamente disipan calor, de forma que producen calentamiento en los dispositivos.

La posibilidad matemática de una computación clásica reversible la ideó Yves Lecerf en 1963; en 1982, Charles Bennett estableció la posibilidad de una máquina de Turing reversible. En otras palabras, para eludir la irreversibilidad inherente a algunas de las más frecuentes puertas clásicas, podían desarrollarse puertas alternativas adicionales que permitirían acometer todo cálculo computacional clásico en sucesivas etapas reversibles. Pero el precio de la mayor eficiencia energética, conseguida al eliminar la disipación de calor, podría ser una mayor duración del procedimiento, al involucrarse en general el acarreo de más bits. La importancia de este descubrimiento para la computación cuántica radica en que, como hemos dicho, todas las puertas cuánticas van a ser reversibles, debido a que la ecuación de Schrödinger es ella misma reversible: su forma matemática es tal que la ecuación nos proporciona la misma evolución temporal si consideramos que el tiempo avanza que si consideramos que retrocede. En términos matemáticos, se dice que la evolución temporal que fija la ecuación de Schrödinger es unitaria, en consecuencia, todas las operaciones que realicemos sobre un qubit, esto es, las puertas cuánticas que diseñemos, han de respetar esa reversibilidad, o sea, corresponder a operaciones unitarias. En esencia, la *unitariedad* de una puerta consistirá en

que se habrá de conservar la normalización del estado cuántico sobre el que se aplica, lo que implica que ha de tener el mismo número de qubits a la entrada y a la salida. Dos puertas cuánticas unitarias elementales son las unarias (entra y sale un solo qubit) identidad, símbolo I, y negación, NOT o FLIPBIT, cuya acción sobre los qubits fundamentales (en general, representaremos la acción de una puerta sobre un qubit por el símbolo ♦) es, respectivamente, dejarlos igual ($I \blacklozenge 0^q = 0^q$; $I \blacklozenge 1^q = 1^q$) o intercambiarlos (NOT ♦ $0^q = 1^q$; NOT ♦ $1^q = 0^q$).

Se dice que un conjunto de puertas cuánticas es universal si recurriendo a ellas es posible implementar, en un número dado de etapas de cálculo, cualquier operación unitaria posible sobre los qubits. En el año 1995, Adriano Barenco y otros autores probaron que, por ejemplo, el conjunto integrado por la puerta cuántica CNOT y cualquier puerta unaria es universal.

Como ejemplo de cómo actúa y se representa una puerta, vamos a explicar el funcionamiento de este operador CNOT, también llamado negación controlada o XOR cuántico. Es un operador binario, de manera que actúa sobre dos qubits (entran dos qubits), y ha de entregar después otros dos (salen dos qubits) porque, como debe ser para toda puerta cuántica, no puede alterar su número (unitariedad). Su acción sobre un par de qubits consiste en que no altera el primero, y cambia o no el segundo dependiendo del estado del primero: si este es 1^q, aplica sobre el segundo el operador negación, que invierte su valor, y si es 0^q, el operador identidad, que lo deja igual. En concreto, pues, sobre los estados de la base computacional para el 2-qubit actúa según:

$$\text{CNOT} \blacklozenge (00)^{(2Q)} = (00)^{(2Q)}$$
$$\text{CNOT} \blacklozenge (01)^{(2Q)} = (01)^{(2Q)}$$
$$\text{CNOT} \blacklozenge (10)^{(2Q)} = (11)^{(2Q)}$$
$$\text{CNOT} \blacklozenge (11)^{(2Q)} = (10)^{(2Q)}$$

En consecuencia, sobre el estado general de un 2-qubit, el operador CNOT realizará la siguiente acción:

$$\text{CNOT} \blacklozenge [\alpha_0 \cdot (00)^{(2Q)} + \alpha_1 \cdot (01)^{(2Q)} + \alpha_2 \cdot (10)^{(2Q)} + \alpha_3 \cdot (11)^{(2Q)}] =$$
$$= \alpha_0 \cdot (00)^{(2Q)} + \alpha_1 \cdot (01)^{(2Q)} + \alpha_2 \cdot (11)^{(2Q)} + \alpha_3 \cdot (10)^{(2Q)}$$

La puerta cuántica binaria CNOT, por lo tanto, al actuar sobre un estado entrante, incluso cuando este fuera no entrelazado, podría acabar entregando a su salida un estado entrelazado, ya que recordemos que la mayoría de las elecciones de valores para las cuatro constantes (α_0, α_1, α_2 y α_3), en la expresión de un 2-qubit general, conducen a un estado entrelazado. Este hecho será muy útil, ya que esos estados entrelazados podrán usarse entonces para teleportar información entre partes distantes de un computador cuántico.

La arquitectura de un ordenador cuántico que se basa en circuitos de puertas cuánticas, que se van aplicando de forma sucesiva a los diversos qubits, es la que ha tenido un mayor desarrollo teórico, al trasladar de una forma directa la imagen de la computación clásica. Construir un ordenador cuántico de esta forma involucraría las siguientes etapas: inicialización de los qubits, es decir, situarlos en unos estados dados de partida; almacenaje de la información en los qubits; realización de las operaciones lógicas sobre ellos, a través de las puertas lógicas; traslado de información entre distintas zonas del dispositivo; lectura de los qubits individualmente, de forma que los estados finales que emerjan sean precisamente los que contienen la información útil para resolver el problema planteado. Ninguna de ellas es trivial.

Se han discutido también otros marcos teóricos que pueden proporcionarnos un ordenador cuántico y que no incluyen la implementación de circuitos con puertas lógicas. Aunque no es la única, sin duda la tecnología alternativa que más se ha desarrollado es la llamada *computación cuántica adiabática* (AQC, por sus siglas en inglés), basada en una cadena de sucesivas interacciones sobre el correspondiente sistema de qubits que se realizan «suavemente», de manera que le van provocando una secuencia de muy pequeñas y débiles modificaciones. Con ello, se consigue que el sistema permanezca «recociéndose», y aunque va cambiando muy lentamente, no experimenta excitaciones hacia

energías superiores, sino que sigue un tipo de evolución que se suele definir como adiabática. La idea es lograr llevarlo hacia la configuración final que se asocia o corresponde a la solución óptima buscada para cada problema planteado, es decir, el estado final que contiene la información deseada. En la AQC se integran algunos prototipos comerciales de ordenadores cuánticos, ya a la venta y, además, vendidos. Los veremos al final de este capítulo; antes, insistiremos en recordar que un ordenador cuántico necesita instrucciones también cuánticas para explotar su potencia.

ALGORITMOS CUÁNTICOS: LA BÚSQUEDA DEL PROCEDIMIENTO IDÓNEO

Un algoritmo es un conjunto ordenado de operaciones que nos permite realizar una tarea, es decir, un proceso ordenado de instrucciones para la resolución de un problema. Los algoritmos se representan mediante diagramas o circuitos, que nos van describiendo mediante una secuencia de puertas cuánticas, ordenadas temporalmente de izquierda a derecha, las sucesivas transformaciones unitarias que se realizan sobre los qubits y que conducirán a ultimar el cálculo acometido. En la figura 3 se representa la forma general que tendría este tipo de diagramas.

Los algoritmos se clasifican en términos de su eficiencia, algo que es difícil de determinar. Por ejemplo, ¿es más eficiente, para el mismo problema, el algoritmo más rápido o el que requiere menos memoria? Depende de lo que se priorice. Así que, en general, se suele hablar de distintas clases de complejidad de un algoritmo; por ejemplo, respecto a la pregunta anterior, hablaríamos de complejidad temporal y espacial, respectivamente. En general, respecto al grado de complejidad temporal de un algoritmo se distinguen varias clases, en función de la relación que guarden los recursos involucrados para la resolución de un problema frente al tamaño del conjunto de datos que se tienen que manejar. Para ello se determinan, por un lado, los recursos consumidos a partir del número de sucesivos pasos temporales o instrucciones requeridos por el algoritmo; por otro, cuán gran-

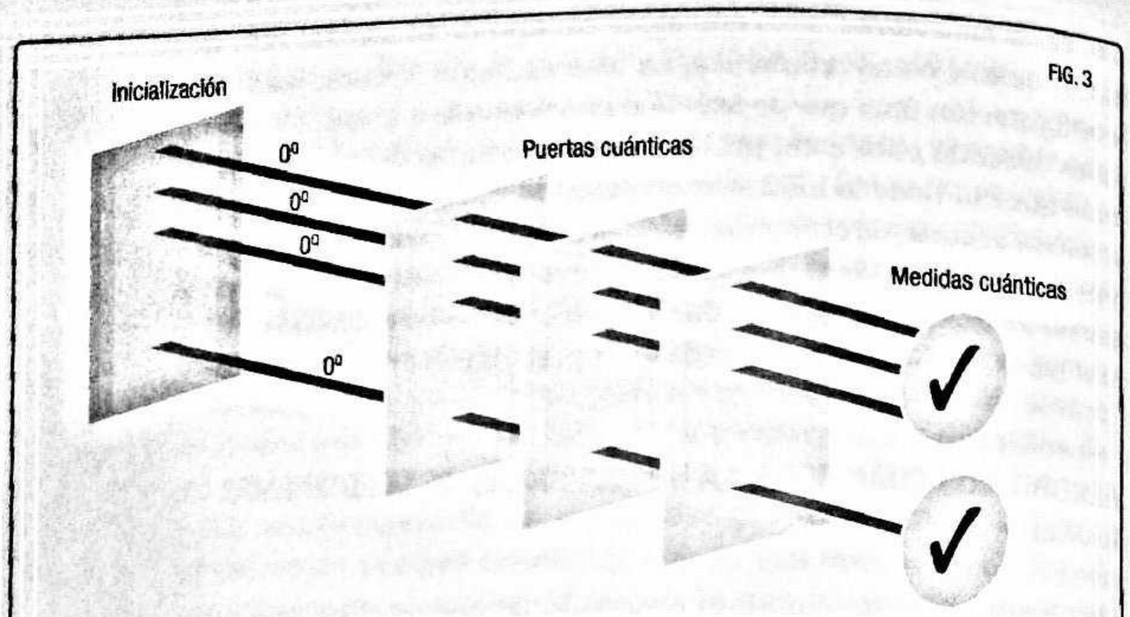


Diagrama general de un circuito cuántico. Se comienza con la inicialización de unos qubits (representados por líneas horizontales); se prosigue con la acción de una serie de puertas cuánticas y se finaliza con la operación de medida o lectura (representada por el símbolo ✔ en un círculo) sobre el correspondiente conjunto de bits abarcados, que colapsa las superposiciones cuánticas.

des son los datos de entrada, a partir del número de bits necesarios para su representación. Obsérvese que la función que relaciona ambas variables no depende del ordenador concreto que vaya a usarse, es decir, en el que vaya a resolverse el problema con el algoritmo analizado.

En general, para que un algoritmo sea eficiente lo que importa sobre todo es que el número de instrucciones necesarias para resolver el problema no se dispare cuando el tamaño de los datos involucrados aumenta. De esta manera, es crucial conocer para cada algoritmo aplicable a un problema concreto en qué clase de complejidad se encuadra, y hay tres clases principales de problemas, según el tipo de los mejores algoritmos disponibles para resolverlos, cada una de las cuales engloba a su vez muchos subtipos. Uno: la clase «tratable», o clase P, cuando el número de instrucciones crece como una función polinómica con el tamaño de los datos (según las diversas potencias de este tamaño: o se mantiene constante, o crece de forma lineal, cuadrática, etc.).

Dos: la clase «algo intratable», NP, cuando, aunque el crecimiento en la demanda de recursos de los algoritmos sea exponencial, sucede sin embargo que, si logramos encontrar una solución, probar que efectivamente lo es sí constituye un problema de clase P. Y, por último, tercera clase: la «por completo intratable», o clase NP-C (NP-completa), con problemas para los que, si encontramos como sea una solución, probar que efectivamente lo es constituye a su vez un problema cuya demanda de recursos crece exponencialmente con el tamaño de los datos de entrada. Para los problemas de esta última clase, la NP-C, en 1971 se formuló el teorema Cook-Levin, según el cual todos pueden considerarse un mismo problema, en el sentido de que, si se consiguiera desarrollar un algoritmo resolutivo que fuera muy eficiente —de la clase P— para un problema de la clase NP-C, entonces resolvería todos los problemas de las dos clases NP. Es decir, las disolvería: dejarían de existir por vaciamiento, ya que todos sus problemas se trasladarían a la clase P. Al año siguiente de publicarse el teorema, Richard Karp elaboró una lista de 21 problemas NP-C, para los cuales demostró esa cualidad de ser en efecto de la clase NP-C (a falta de un algoritmo polinómico panacea).

Pongamos algunos ejemplos de problemas y sus complejidades. Si queremos multiplicar dos números de N dígitos, la complejidad de los algoritmos disponibles crece con el cuadrado del número de dígitos: decimos que el problema tiene una complejidad (temporal) de orden N^2; se trata de un problema «tratable» (clase P). En cambio, el problema de la factorización de un número de N dígitos, descomponerlo en sus factores primos —escribir algo como $15=3\cdot5$; $70=2\cdot5\cdot7$, etc.— es un problema «algo intratable»: su complejidad crece exponencialmente, lo que quiere decir que es de orden muy superior al polinómico. Suponiendo que tardáramos un mes en factorizar un número de 130 dígitos, con los mismos medios tardaríamos 10^{10} años —en torno a la edad del universo— para factorizar uno de 400 dígitos. Es precisamente este hecho, como veremos en el capítulo sobre criptografía, lo que garantiza la seguridad de muchas de las comunicaciones cifradas actuales, ya que se necesitan enormes redes de supercomputadoras clásicas, trabajando cooperativamente durante muy

largos periodos de tiempo, para que los mejores algoritmos logren las factorizaciones precisas para descubrir las claves con el número de dígitos que se suelen usar hoy en día en los principales sistemas clásicos de cifrado. Por último, un famoso problema NP-completo es el del «coloreado de gráficos»: dados tres colores y un gran mapa de muchas regiones contiguas, hay que colorearlo usando solo tres colores y de manera que nunca dos países con frontera común tengan el mismo color. Si alguien ideara un algoritmo óptimo, de orden polinómico, para resolver un problema NP-completo, se haría millonario seguro. La creencia general es que no vamos a verlo (pero no se ha probado la imposibilidad absoluta de tal logro), así que este famoso desafío intelectual, el «problema NP-C versus P», sigue abierto.

Sería fantástico poder afirmar que la computación cuántica nos va a permitir acometer eficientemente, gracias al paralelismo que proporcionan las superposiciones, cualquier problema que en computación clásica es hoy algo intratable, a falta de un algoritmo que haga el problema tratable. Pero existen temores fundados de que ello no va a ser así, ya que, al ser leídas —sometidas a medida—, las superposiciones cuánticas «escupen» un solo resultado, de entre todos los superpuestos (el famoso colapso cuántico). De modo que, independientemente de que la tecnología logre construir en el futuro poderosas máquinas cuánticas, domeñando la decoherencia y consiguiendo la escalabilidad en su diseño requerida, nos seguirían faltando algoritmos cuánticos para que algunos de esos problemas NP dejaran de serlo, especialmente los de clase NP-completa. Esos algoritmos deben desarrollar estrategias para aprovechar las novedades principales de la física cuántica respecto a la clásica, como los estados superpuestos —el paralelismo— y el entrelazamiento. Dicho en otras palabras: no podemos esperar que el paralelismo cuántico nos permita resolver por sí solo los problemas para los que la computación clásica es poco eficiente. Ahora bien, ese paralelismo cuántico, en definitiva, las leyes de la física cuántica, ¿no pueden abrir pasos a nuevos y más eficientes algoritmos, específicamente desarrollados para incorporar y explotar como ventaja las leyes del mundo cuántico, en el contexto de algunos problemas

específicos? La respuesta es afirmativa: algunos de esos algoritmos, muy pocos, ya existen, algoritmos cuánticos que convierten problemas que son en computación clásica algo tratables (clase NP con test de solución P), en problemas tratables, de clase P, en computación cuántica. La clase BQP de problemas se define como la integrada por todos los problemas para los que la computación cuántica ofrecería una resolución en tiempo polinómico, esto es, problemas que son de clase P en computación cuántica. Lamentablemente, se cree que la mayoría de los problemas NP, y todos los NP-C, van a quedar fuera de ella.

Los dos principales algoritmos cuánticos desarrollados hasta la fecha han sido el de Shor y el de Grover. El primero, ideado por Peter Shor en 1994, tiene por objetivo factorizar un número entero de N dígitos como producto de dos enteros menores, o mostrar que es primo, en su caso, y lo consigue consumiendo recursos temporales que crecen según un orden polinómico. De modo que, puesto que los mejores algoritmos clásicos de factorización necesitan un tiempo que crece de forma exponencial con la raíz cúbica del número N de bits, el algoritmo de Shor triunfa al conseguir un tiempo proporcional al cubo de dicho número, con un uso de memoria del orden del logaritmo de N. Es un algoritmo de tipo probabilístico: proporciona solo una probabilidad (alta) de encontrar la respuesta buscada; en caso de fallo, se debe repetir de forma sucesiva.

Hay que tener en cuenta que, según veremos en el capítulo de criptografía, la seguridad de las actuales comunicaciones cifradas radica en que los mejores algoritmos clásicos desarrollados hasta la fecha para el problema de la factorización son de clase NP, así que convertir el problema en clase P dinamita esa seguridad (tranquilidad, todavía falta el ordenador cuántico en que ejecutar este algoritmo para números grandes). No es de extrañar, pues, que la publicación de este algoritmo de Shor supusiera un gran revulsivo hacia la investigación en pro de la computación cuántica: se estima que, de disponerse de un computador cuántico universal, con el número de puertas lógicas requeridas, con este algoritmo se lograría factorizar un número de 130 dígitos, por ejemplo, en segundos. Hasta el presente, puesto que solo se dispone de

prototipos muy limitados de ordenadores cuánticos, con unos pocos qubits, únicamente se ha podido aplicar el algoritmo para números muy pequeños. Como dato ilustrativo: la factorización del número 15 necesita en principio de 12 qubits, y para llevar a cabo una factorización no elemental se necesitaría un computador cuántico de miles de qubits, incluyendo los necesarios para la imprescindible corrección de errores, mientras que hoy los mejores prototipos apenas superan la decena de qubits. El algoritmo, por cierto, también es aplicable al problema del logaritmo discreto (de forma simple: dados g y a, encontrar el entero k tal que $g^k = a$), que es la base para otros sistemas criptográficos actuales.

En 1997, Lov Grover presentó un algoritmo para resolver búsquedas no estructuradas, esto es, el tipo de búsqueda en una base de datos que no está ordenada en términos de la información conocida. Por ejemplo, buscar el nombre de una persona en una guía telefónica con los titulares de las líneas ordenados alfabéticamente, a partir de un número de teléfono. Se trata también de un algoritmo probabilístico, que conlleva una sustancial ganancia de recursos —aunque la mejora en este caso no es exponencial— frente al mejor algoritmo clásico disponible. Este algoritmo consigue ingeniosamente que las amplitudes de la superposición cuántica que no contienen la respuesta correcta se vayan minimizando, mientras que se refuerza la asociada a la correcta, de forma que, en la lectura o medición final, hay alta probabilidad de éxito. Unos datos: si clásicamente en una guía de N entradas habría que realizar un número de búsquedas del orden de N (leer al menos $N/2$ entradas para alcanzar una probabilidad del 50% de localizar al titular de un número de teléfono específico, que sabemos que está en la guía), con el algoritmo de Grover el número de búsquedas requeridas se reduce al orden de $\sqrt{N}$.

ORDENADORES CUÁNTICOS REALES: ¿EXISTEN YA? ¿SE PUEDEN COMPRAR?

Richard Feynman afirmó en 1982 que para simular determinados fenómenos cuánticos, una máquina clásica implicaría de forma ineludible una demanda de recursos temporales con crecimiento exponencial respecto al tamaño de los datos. De forma que, para la simulación general de procesos cuánticos, y también, como hemos visto, para algunos otros problemas específicos, está claro que se requerirán computadoras cuánticas: dispositivos de cálculo que contengan partículas en estados cuánticos, estados de superposición y entrelazados, y que permitan operar sobre ellos según algoritmos cuánticos. La investigación hacia la construcción de estas máquinas cuánticas es imparable y ha generado ya, como vamos a ver a continuación, prototipos operativos, aunque todavía con muy pocos qubits. Y es que la tecnología desarrollada para la construcción de ordenadores cuánticos está en sus inicios, así que tardaremos en verlos en los grandes almacenes (si es que los vemos, lo que es muy dudoso, y no solo porque no prometen ser baratos). Es una tecnología que afronta enormes problemas; a continuación vamos a detallar algunos de los principales, tan solo una pequeña selección de una larga lista.

> El propósito de la computación es la comprensión, no obtener números.
>
> **Richard Hamming**

En primer lugar, el fenómeno de la decoherencia, que es como se denomina el proceso por el que una superposición cuántica se desploma, produciéndose su colapso hacia un estado final no superpuesto (el qubit general $a \cdot 0^Q + b \cdot 1^Q$, por ejemplo, se convierte en uno fundamental, el 0^Q o el 1^Q). Si se quiere evitar, resulta imprescindible aislar escrupulosamente del entorno los frágiles estados cuánticos superpuestos, para evitar su colapso a resultas de cualquier mínima interacción incontrolada con el medio. Por tanto, se necesita mantener el sistema a temperaturas muy bajas, lo que lleva a pensar que, en un futuro, más que multiplicarse los ordenadores cuánticos en los hogares, solamente se dispondría de algunos que, por su elevado coste de mantenimiento, solo algunas grandes corporaciones podrían mantener: los usuarios trabajarían interaccionando con ellos desde sus lugares de trabajo (una «nube cuántica»). Y es que las superposiciones cuánticas y los estados entrelazados son muy delicados: las interacciones del entorno los destruyen, provocando la pérdida de información

o, como mínimo, corrompiéndola, introduciendo errores. Con respecto a esto último, hace falta conseguir cierta tolerancia a los inevitables errores. Hay que incorporar un control de errores, puesto que se van a producir forzosamente, como en la computación clásica. Pero si en el procesado y almacenaje de información clásica se puede recurrir para ello a las técnicas redundantes, en cuántica es imposible, ya que no se pueden duplicar los estados para repetir así los registros de una misma información (por el teorema de no duplicación cuántica). Hoy en día, la investigación en técnicas de corrección de errores es un campo abierto y en continuo desarrollo, pero también todavía en sus inicios.

Otro problema que se presenta es conseguir una interconectividad y una escalabilidad adecuadas. Respecto a la primera, los procesos de información cuántica se desarrollan a escalas de tiempo y tamaño que han de conectarse con la escala macroscópica de los observadores, incluyendo en estos últimos no solo a los manipuladores humanos, sino a los dispositivos de escala clásica, como electrodos de control y detectores, inevitables en las etapas de entrada y salida de datos. En un mismo chip, pues, habrán de aprender a convivir, conectados, el circuito cuántico y la electrónica clásica. Respecto a la segunda, se necesita un diseño que permita la ampliación practicable del dispositivo para procesar más y más qubits, con muchas puertas cuánticas encadenadas. Los prototipos actuales consiguen, muy esforzadamente, manejar apenas unos pocos qubits.

Se plantean muchos más interrogantes. ¿Cómo construir en la práctica un ordenador cuántico? ¿Cómo construir varias puertas lógicas cuánticas y cómo conectarlas entre sí, creando redes cuánticas cada vez más complejas y extensas? ¿Cómo mantener el sistema global bien aislado del entorno, inicializar los qubits y leer los resultados finales? ¿Cómo, especialmente si se adopta una tecnología adiabática, mantener todo el sistema a las bajísimas temperaturas requeridas para que el sistema manejado no sufra una alteración indebida de su estado? Por supuesto, en la práctica todo esto es muy difícil, de modo que la computación cuántica, operativamente eficiente, parece muy lejana en el horizonte. El ingenio y la pericia de los investigadores, pese a ello, ha ido desarrollando pequeños —en cuanto a número de qubits— prototipos, utilizando diversas tecnologías. A continuación exponemos una breve y mínima selección de avances, agrupados por clase de tecnología.

En primer lugar, hay que destacar la tecnología que incluye las trampas de iones, en la que, como ya vimos, se confinan iones atómicos en una región del espacio mediante la aplicación de campos electromagnéticos, manteniéndolos separados entre sí por distancias del orden de pocos micrómetros. Una vez confinados los iones, se actúa sobre ellos con los adecuados láseres, consiguiendo enfriarlos y que permanezcan en el estado de energía más bajo posible para el sistema. Desde que Ignacio Cirac y Peter Zoller lo propusieran en 1995, se han desarrollado diversos prototipos de ordenador cuántico con trampas iónicas, todavía con pocos qubits. Probablemente es la tecnología que antes parece prometer una cierta escalabilidad, de modo que quizá pronto veamos logros experimentales que manejen varias decenas de qubits. Los qubits se van a implementar sobre los iones confinados, que pueden situarse cada uno, individualmente, en dos estados posibles, 0^{ϱ} y 1^{ϱ}, pudiendo estimularse las transiciones entre ellos de nuevo por la acción de láseres. Para implementar una puerta lógica, por ejemplo, puede hacerse uso de «toques» con un láser sobre los iones: estos absorben un fotón y se desplazan hacia la derecha, hacia la izquierda, o hacia los dos lados a la vez. A partir de estas acciones sobre dos iones en una hilera se puede implementar una puerta cuántica: es lo que han conseguido en la Universidad de Innsbruck Rainer Blatt y su equipo, quienes publicaron en 2003 en *Nature* la realización de una puerta CNOT con una hilera de iones de calcio en una trampa. En 2005 lograron entrelazar hasta ocho iones de calcio en su trampa, produciendo un primer *qubyte* (conjunto de ocho 1-qubits). Este mismo equipo publicó en junio de 2016 un algoritmo cuántico para la simulación en su trampa de iones de calcio de algunos procesos fundamentales de interacción entre partículas elementales.

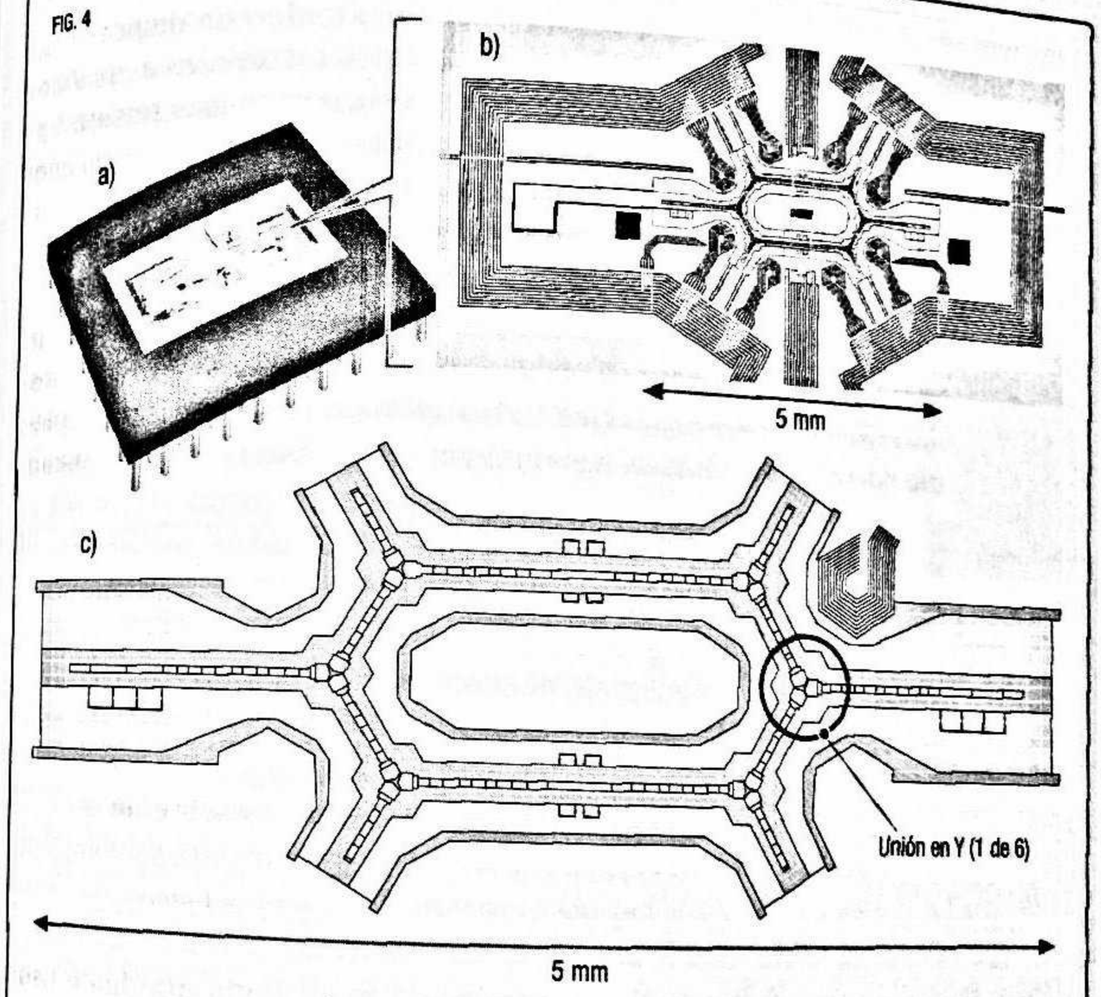
En 2009, David Hanneke y un equipo del NIST (*National Institute of Standards and Technology*, Instituto Nacional de Normas

y Tecnología de los Estados Unidos), en Colorado, desarrollaron el primer procesador cuántico efectivamente programable, un sistema con dos puertas cuánticas que constituían juntas un conjunto universal, por lo que —idealmente— podía ejecutar cualquier cálculo o conjunto de instrucciones. La implementación se realizó sobre un par de átomos de berilio en una trampa; la información se almacenaba sobre ellos mediante láseres ultravioleta, que fijaban el estado cuántico del par, mientras que se usaban campos eléctricos para desplazar los átomos por la trampa. La figura 4 muestra un esquema de este tipo de dispositivo. En marzo de 2016, investigadores del MIT (*Massachusetts Institute of Technology*, Instituto Tecnológico de Massachusetts) y de la Universidad de Innsbruck publicaron en *Science* el diseño de una trampa con cinco átomos con la que han logrado aplicar el algoritmo de Shor y resolver $15 = 3 \cdot 5$. El sistema está diseñado para permitir su escalabilidad, de modo que se puedan añadir más átomos y más láseres, lo cual supondría poder abordar factorizaciones de números mayores. Isaac Chuang, uno de sus desarrolladores, quien ya en 2001 participó en la primera implementación experimental del algoritmo, afirmaba con optimismo en la página web del MIT:

> Hemos demostrado que el algoritmo de Shor, el algoritmo cuántico más complejo desarrollado hasta la fecha, se puede realizar de una forma en la que basta con aplicar más tecnología en el laboratorio para tener un computador cuántico mayor. [...] Puede que cueste un montón de dinero construirlo —no lo construiremos y lo pondremos sobre nuestros escritorios a corto plazo—, pero ahora se trata ya más de un esfuerzo de ingeniería que de un problema físico.

En segundo lugar, cabe destacar la tecnología que hace uso de la resonancia magnética nuclear: dispositivos que recurren a los espines nucleares moleculares para construir los qubits. Un logro crucial fue realizar por primera vez, en 2001, el algoritmo de Shor sobre este tipo de dispositivos en una investigación realizada por Lieven Vandersypen y sus colaboradores, un equipo

del centro de IBM en California y la Universidad de Stanford. Hacían uso de una disolución molecular en cuyo seno se albergaban siete núcleos de espín 1/2, que utilizaban para implementar los qubits, a partir de dos estados moleculares distinguibles conseguidos aplicando campos magnéticos. Exponiendo las moléculas a pulsos de radio con frecuencias específicas, lograban inicializar los estados y generar varias puertas cuánticas. El

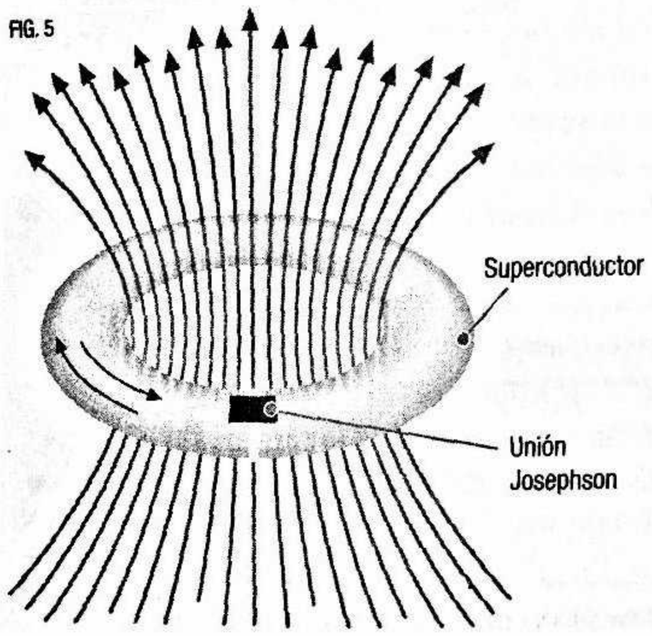


Microtrampa de superficie de iones diseñada por el NIST en 2010. La trampa se monta sobre una PGA (*Pin Grid Array*, matriz de rejilla de pines) (a). En la región activa de la trampa (b) se observan seis uniones en Y formando un anillo hexagonal (c), a través de las cuales se logró transportar iones de magnesio. El dispositivo está ideado para ser escalable hacia un tamaño en principio tan grande como se quiera, por lo que constituye un gran avance hacia la construcción de circuitos cuánticos manejando muchos qubits.

problema con estos dispositivos es que los espines se invierten fácilmente por la acción de los campos magnéticos de las partículas del entorno, así que es importante aislarlos bien, para lo cual se han empleado técnicas como las de embeberlos en silicona purificada.

En tercer lugar, tenemos la tecnología de dispositivos sólidos, como átomos en hileras de pozos de potencial creados por la adecuada conjunción de láseres, o electrones en el seno de materiales superconductores, que tienen la propiedad de no ofrecer apenas resistencia al paso de la corriente eléctrica cuando su temperatura se baja lo suficiente. En estos materiales es posible implementar los qubits vía corrientes eléctricas que siguen bucles cerrados en los dos sentidos posibles, según se muestra en la figura 5. El grupo de John Martinis, en la Universidad de California, ha logrado fabricar qubits de esta forma, manteniéndolos durante tiempos del orden de 50-100 μs. En general, un dispositivo que implementa qubits a partir de este tipo de proceso, a veces denominado SQUID (sigla de *Superconducting Quantum Interference Device*, dispositivo superconductor de interferencia cuántica; en inglés *squid* significa «calamar»), dispone de

FIG. 5



Esquema de una unión Josephson, una zona aislante muy fina colocada en un anillo de material superconductor, que es sometido primero a un campo magnético (representado por las flechas que atraviesan el anillo) y luego enfriado. El resultado es que se induce en él una corriente en bucle, que atraviesa la unión por efecto túnel y que, bajo la adecuada preparación, puede colocarse en un estado cuántico de superposición de dos estados que describen sendas corrientes en los dos sentidos de circulación posibles, horario y antihorario (representadas por las flechas negras). Este tipo de estados se pueden usar para la implementación de qubits.

dos semiconductores, separados por una fina lámina aislante, en un tipo de unión bautizada *unión Josephson*, que los electrones no solo son capaces de atravesar, constituyendo corrientes en los dos sentidos, sino también de hacerlo en estados correspondientes a superposiciones de esos dos sentidos de la corriente. En 2016, un equipo conjunto de investigadores de Google y de varias universidades anunció la simulación computacional correcta de la estructura de una molécula de hidrógeno —diatómica—, utilizando una estructura de dos qubits superconductores que afirmaban que admitiría una escalabilidad directa, lo que permitiría la simulación futura de moléculas mayores, inabordables hoy en día con ordenadores clásicos. Se sugiere que esta tecnología ofrecerá en general la ventaja de una escalabilidad más fácil; de momento, la computación cuántica adiabática ha hecho uso de estos SQUID, proporcionándonos los primeros computadores cuánticos comercializados.

> Ya está próxima la era de los químicos computacionales, en la que cientos si no miles de químicos trabajarán con ordenadores en lugar de hacerlo en el laboratorio.
>
> ROBERT MULLIKEN

En cuarto lugar, no menos importantes aunque más difícilmente escalables, están los dispositivos ópticos. Los progresos en óptica cuántica han hecho que muchos la consideren el campo idóneo para realizar la computación cuántica: qubits fotónicos. Se han publicado numerosísimas implementaciones de puertas lógicas fotónicas u ópticas. Jeremy O'Brien y su equipo, de la Universidad de Queensland, lo hicieron para la puerta CNOT en 2003, y después consiguieron reunir cientos de estas puertas en una pieza de silicona milimétrica, incorporando guías de onda también de diámetro micrométrico (las guías de onda son como cables huecos por cuyo interior se conduce la luz, evitando así las frecuentes interferencias que se producen en la trasmisión aérea). Asimismo, son ya muchas las publicaciones que han mostrado diseños de circuitos con puertas fotónicas, capaces de ejecutar los algoritmos cuánticos. En 2009, O'Brien, con un equipo de la Universidad de Bristol, publicó en *Science* la factorización $15=3\cdot5$ con el algoritmo de Shor, mediante un chip óptico

LA COMPUTACIÓN DEL FUTURO

El funcionamiento de los ordenadores cuánticos se basa en la superposición y entrelazamiento de estados, dos conceptos fundamentales de la mecánica cuántica. En computación cuántica, las puertas lógicas operan con qubits, que pueden tomar valores 0 o 1 y también la superposición de ambos. Esto permite realizar múltiples operaciones al mismo tiempo y constituye una de las grandes ventajas de los ordenadores cuánticos respecto de los clásicos.

En la figura, algunos rayos de luz inciden sobre un cristal químicamente dopado y cuyo tamaño es de pocos nanómetros, como los que se usarán en el diseño de computadores cuánticos ópticos. Esta tecnología ha conseguido desarrollar circuitos integrados fotónicos, un primer paso hacia la requerida escalabilidad de los dispositivos.

de silicona, que incluía finas guías de onda. En 2012, otro equipo presentaba en *Nature Photonics* la factorización de $21 = 3 \cdot 7$ con un dispositivo óptico.

GRANDES EMPRESAS, GRANDES PROYECTOS

En 2014, Google reclutó un equipo de científicos de la Universidad de California para integrarlos en un proyecto destinado a construir un ordenador cuántico, con la vista puesta en un plazo de dos o tres décadas. Está claro que solo quienes disponen de suficientes fondos pueden invertir tanto capital pensando en tan larga producción de rentabilidades. Contratar a buenos investigadores en física teórica para reconvertirlos en lo que han dado en llamar «ingenieros cuánticos» parece el primer paso. Microsoft e IBM también están preparados para participar en la carrera de la computación cuántica, junto con numerosos institutos y universidades repartidos por el mundo. En cualquier caso, la tecnología de la computación cuántica está hoy en sus inicios, como declaraba Martinis en una entrevista en 2014, «estamos en algún lugar similar al que se encontraba la computación clásica entre la invención del transistor y la de los circuitos integrados».

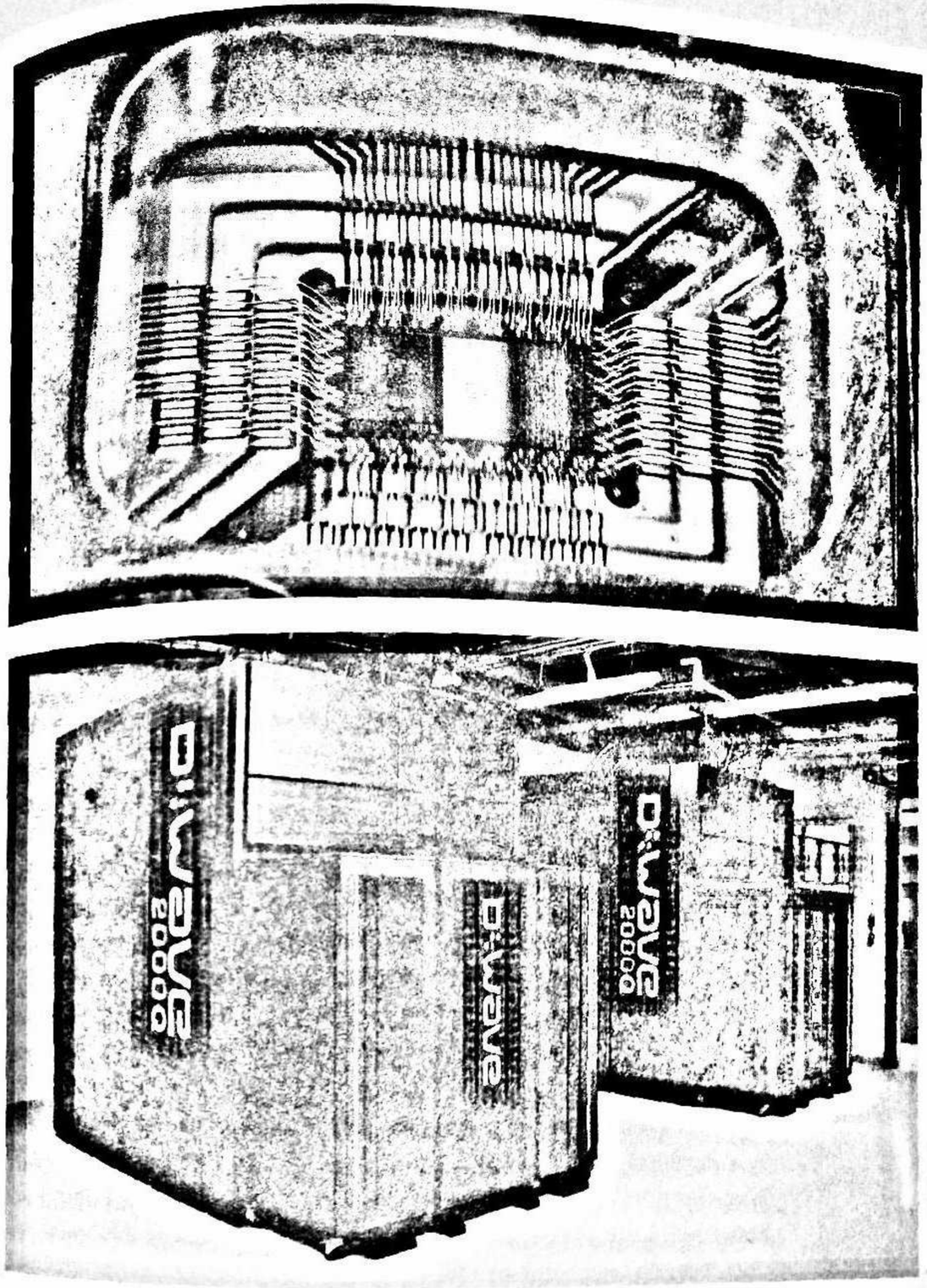
IBM no solo dispone ya de un prototipo de ordenador cuántico universal, con qubits implementados sobre dispositivos SQUID y tecnología adiabática, que debe ser preservado a bajísimas temperaturas y que es capaz de trabajar con cinco qubits, construido en su laboratorio de Yorktown Heights, Nueva York, sino que lo ha puesto en la nube, a disposición del público general. En palabras de la compañía: «Poniendo a disposición de todo el mundo a través de internet uno de estos ordenadores, IBM se asegura [...] de que cientos de investigadores, ingenieros y programadores lo van a probar, encontrando fallos y proponiendo mejoras». Basta con solicitarles una cuenta de trabajo para tener la satisfacción, por ejemplo, de sumar —con muy pocos dígitos— en un ordenador cuántico. Una fantástica campaña de promoción, que pretende también ayudar a muchos investigadores del ramo que ni por ensueño podrían tener acceso a un dispositivo así en sus instituciones. IBM pretende ampliar los qubits disponibles hasta 50, en una primera fase, y luego hasta 100.

Por supuesto, no podemos acabar sin mencionar a la primera empresa que puso a la venta, en 2011, un supuesto ordenador cuántico: la canadiense D-Wave Systems. En 2007 presentaron en público el prototipo D-Wave Orion, de 16 qubits, en un acto cargado de oscuridad, ya que la información sobre la máquina que divulgaron —a diferencia de la transparencia con que IBM presentó su computador— no permitió a los investigadores una inspección y un juicio conclusivo sobre el carácter cuántico o no de las entrañas del dispositivo. Por ello, le acompañó una polémica sobre si realmente debía ser considerado un ordenador cuántico; el hecho es que los principales expertos en tecnología cuántica adiabática lo han considerado más bien un simulador clásico de esa tecnología que un computador cuántico real. El punto crucial es que se sospechó que en realidad no albergaba en su interior estados de qubits superpuestos y entrelazados, sino que se trataba solo de un conjunto de qubits superconductores bien interconectados en celdas y redes, que se comportarían en definitiva como los análogos bits clásicos, permitiendo simular el característico y verdadero comportamiento cuántico probabilístico. En cualquier caso, en 2011 salió a la venta el D-Wave-1, un monolítico cubo de 45 m^3 de volumen, ya con un procesador de 128 qubits, que se muestra en la fotografía superior de la pág. 113. Lanzado al módico precio de diez millones de dólares, fue adquirido por la multinacional aeroespacial Lockheed Martin. En 2012, el D-Wave-2, al mismo precio que su antecesor, alcanzó los 512 qubits, y en 2013 se anunció que sus compradores, la NASA y Google, colaborarían usándolo en un proyecto de investigación sobre inteligencia artificial. Los mismos clientes adquirieron el siguiente modelo, que salió en 2015: el D-Wave 2X, una máquina con ya más de mil qubits. A comienzos de 2017, la empresa puso a la venta un nuevo modelo, el D-Wave 2000Q, con 2000 qubits, cuyo aspecto es el que muestra la fotografía inferior de la pág. 113.

> No temo a los ordenadores. Temo quedarme sin ellos.
>
> ISAAC ASIMOV

Los computadores D-Wave usan tecnología adiabática —distinta a la más frecuente y desarrollada teóricamente de circuitos y puertas lógicas—, y han de ser mantenidos a unos pocos milikelvin, unas bajísimas temperaturas que preservan los qubits superconductores, implementados como bucles de corrientes, en sus estados más bajos en energía. Esto los hace más resistentes a las interferencias provenientes del exterior y minimiza la presencia de errores. Por la tecnología usada, no ofrecen gran eficiencia —para gran alivio de muchos— en el problema de factorización de números grandes, pero han mostrado una enorme eficacia en su aplicación a otros problemas muy interesantes, como planes de vuelos en aviación, reconocimiento de voz, traducciones, etc. (y también en la resolución de sudokus, por cierto).

La incredibilidad y la controversia iniciales se reforzaron cuando los computadores no mostraron la mayor eficacia o ganancia en velocidad de cálculo respecto a los competidores clásicos que se había pregonado en algunas pruebas; además, la compañía se seguía mostrando reacia a dar información suficientemente detallada sobre su tecnología en los foros científicos. Sin embargo, con los años parece que la tempestad ha ido amainando, y de hecho se han empezado a publicar aplicaciones resueltas sobre los computadores D-Wave, en diversos campos —desde la secuenciación de ADN a los mercados financieros—, que han aprovechado estos dispositivos con éxito, exhibiendo una ganancia considerable de rapidez frente a los computadores clásicos. Especialmente destacable a favor de los D-Wave fue que en 2012 un grupo de investigadores de la Universidad de Harvard resolviera el problema de la configuración fundamental de una proteína con seis aminoácidos, en un cálculo que incluyó casi 10 000 intentos, de los que solo 13 concluyeron con éxito. Además, en muchas de las ocasiones fallidas se lograron buenas soluciones, aunque no la óptima deseada. El cálculo involucró hasta 81 qubits superconductores; dada su complejidad, fue considerado un enorme éxito de la biofísica computacional en versión adiabática cuántica, frente a la simulación y optimización clásicas. Pero que una máquina sea más eficaz no la convierte en una máquina cuántica.



Arriba, chip Rainier, de D-Wave Systems, un ordenador cuántico adiabático de 128 qubits. Abajo, ordenadores D-Wave 2000Q. Este modelo, de 2 000 qubits, se puso a la venta a comienzos de 2017.

En 2014, un equipo, dirigido por Matthias Troyer, de la Universidad de Zúrich, concluyó sobre la máquina de Lockheed que presentaba indicios reales de conducta cuántica; en una entrevista tras el revuelo que causó su artículo, afirmaba: «[D-Wave] es un prototipo que resuelve problemas específicos usando mecánica cuántica. No es un ordenador cuántico universal que pueda hacer cualquier cosa. Pero es un dispositivo especializado, que puede ser llamado computador cuántico». Parece, pues, que algunos escépticos se van convenciendo, pero solo en el limitado sentido apuntado por Troyer. Scott Aaronson, profesor de ciencia de la computación en el MIT y autoproclamado cabecilla de los escépticos sobre la naturaleza cuántica de los chips D-Wave, aunque admitió que esos resultados podrían constituir un indicio a favor de la naturaleza cuántica de los D-Wave, no ha dejado de advertir contra ellos. Para él, siguen sin ser computadores cuánticos generales, y por eso no pueden acometer el problema de la factorización de números grandes, esto es, aplicar el algoritmo de Shor. De modo que, en su opinión, la tecnología elegida por la compañía canadiense es solo, quizá, un buen negocio, que está ofreciendo eficacia para algunos problemas, pero a un precio que a lo mejor no merece la pena. Y es que, afirma también Aaronson, si hubieran elegido el más esforzado camino de la tecnología universal de puertas lógicas, habrían hecho una aportación científica al desarrollo de la computación cuántica más sustanciosa, aunque quizá no comercializable tan pronto. En cualquier caso, hay que decir que con el tiempo se ha ido produciendo una moderación en las críticas, a la espera de futuros avances y comprobaciones.

A finales de 2015, Google hizo públicos unos experimentos sobre el D-Wave 2X, proclamando haber conseguido un factor de ganancia de velocidad de 100 millones respecto a la computación clásica de esos mismos problemas, con lo que pretendía dejar establecido que se trataba, en efecto, de un ordenador cuántico. Pero tampoco convencieron a los críticos: se adujo de nuevo que, aunque el D-Wave fuera de naturaleza cuántica en el sentido de, por ejemplo, explotar el efecto túnel y contener qubits, eso no lo convertía en el computador cuántico universal, ya que no estaba claro que su tecnología pudiese considerarse capaz de abordar

todos los problemas factibles para una máquina de circuitos y puertas. En definitiva, aunque todavía no hayan sido aceptados de forma unánime como auténticos ordenadores cuánticos, por el momento están demostrando ser máquinas cuánticas que proporcionan ganancias de velocidad que permiten resolver con mayor eficiencia (al menos en tiempos de computación, en costo es otra cosa) ciertos tipos de problemas, esencialmente los de optimización, en los que se busca la mejor solución que cumple la mayoría de varios criterios contrapuestos concurrentes (como encontrar el mejor itinerario para un vuelo, por ejemplo). Pero los críticos insisten en que, incluso en los problemas específicos para los que están indicados, no está claro que siempre aporten mayor eficacia; además, para abordar más problemas de ese tipo especial, se necesita que aumenten bastante los qubits manejados, algo que constituye un desafío en toda regla para el que no hay certeza de éxito. Geordie Rose, fundador de D-Wave en 1999, ya afirmó en 2013: «Estamos absolutamente seguros de que podemos construir la siguiente generación de este dispositivo, pero no tenemos absolutamente ninguna idea sobre cuán bien funcionará». Hasta la fecha, la empresa está comercializando casi cada dos años un nuevo modelo que dobla el número de qubits del anterior.

> La física es el sistema operativo del universo.
>
> STEVEN GARMAN

Respecto al progreso hacia la construcción de un ordenador cuántico de muchos qubits mediante el modelo universal de circuitos y puertas lógicas —lo que muchos ven como la auténtica computación cuántica del futuro, la que explotará a fondo las ventajas de las leyes cuánticas—, el investigador O'Brien declaraba recientemente: «Sería para mí un gran disgusto si en diez años no tuviéramos una máquina capaz de factorizar un número de 1000 bits, es decir, involucrando millones de qubits». Es sin duda un pronóstico muy optimista que, lamentablemente, no es compartido por la mayoría de los especialistas, que creen que probablemente tardarán en llegar, al menos, dos décadas, o más... si es que llegan. El mundo cambiará entonces, como cambió con la computación clásica.

CAPÍTULO 4

Criptografía cuántica

La información es poder, y el secreto de las comunicaciones garantiza la pervivencia del poder... y de la resistencia a él. No ajena a las humanas intrigas, la combinación de técnicas clásicas y cuánticas permite avanzar hacia un intercambio de mensajes cada vez más seguro.

El diccionario de la Real Academia Española define la criptología como el «estudio de los sistemas, claves y lenguajes ocultos o secretos». Podemos distinguir en esta disciplina entre la *esteganografía* o comunicación secreta mediante un mensaje oculto, y la *criptografía*, que definiremos como la técnica de cifrar cierta información para que se pueda transmitir preservando su secreto. La diferencia esencial entre ellas es que la primera pretende ocultar el propio mensaje —por ejemplo, usando tinta invisible u ocultando una imagen digital enmascarando sus bits componentes entre los bits de otras—, mientras que la segunda pretende sobre todo ocultar el significado del mensaje, codificándolo en un criptograma de manera que, aunque sea interceptado, no pueda ser leído. A ellas se añade el *criptoanálisis*, encargado de intentar romper los códigos usados en criptografía, con el fin de tener acceso a la información que se ha pretendido reservar. Como vamos a ver, la física cuántica va a permitir aumentar la seguridad de las comunicaciones, porque nos va a proporcionar garantía respecto a si el mensaje que recibimos ha sido interceptado, es decir, sometido a criptoanálisis, antes de llegar a nosotros.

LA CRIPTOGRAFÍA CLÁSICA Y SU SEGURIDAD

La criptografía comenzó siendo considerada un arte; se transformaría en disciplina científica al trabarse con la matemática y la computación. Su origen puede remontarse al menos hasta el siglo V a.C., cuando los espartanos utilizaron la *escítala*, un primer sistema de criptografía por transposición, es decir, que oculta el significado de un texto alterando el orden de las letras. Un ejemplo lo proporciona el denominado cifrado César, en el que cada letra se sustituye por la que le sigue en el correspondiente alfabeto un número establecido de posiciones; si en este contaje se alcanza la última letra (la *z*), se prosigue por la primera (la *a*). Hay tantas claves posibles como letras tenga el alfabeto que se emplee; la de clave 3 (desplazamiento de tres posiciones) fue la usada por Julio César, correspondiendo a la siguiente tabla de sustituciones, donde la primera fila indica la posición; la segunda, las letras del mensaje original, y la tercera, las del mensaje cifrado:

Lo que no quieras que sepan muchos no lo digas a nadie.

JUAN EUSEBIO NIEREMBERG

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C

Este sencillo método, cuyo criptoanálisis conduce rápidamente a su ruptura o descifrado, corresponde a la fórmula matemática:

$$C(x) = x + 3 \pmod{26},$$

que nos indica que el carácter $C(x)$ que va a sustituir al carácter x del texto plano o sin cifrar (que escribiremos en minúsculas), para formar el criptograma (en mayúsculas), va a ser el que ocupa en un alfabeto de 26 caracteres la posición del x, aumentada en tres unidades; si resulta un número mayor que 25, se le resta 26. Así pues, el símbolo «mod», el *módulo*, indica el número de caracteres de que consta el alfabeto utilizado. Asignado un número, del

0 al 25, a cada una de las letras en que está escrito nuestro mensaje plano, la fórmula nos permite obtener rápidamente su codificación. Por ejemplo, vamos a obtener el criptograma para la oración o mensaje «Ya vive oculta», con ayuda de la tabla de sustituciones anterior. Aplicamos la fórmula a cada letra:

$$C(\text{y}) = 24 + 3 \pmod{26} = 27 \pmod{26} = 1,$$

luego sustituimos la letra *y* por la *B* (ya que 27 es mayor que 25, se le resta 26, obteniendo 1, que es la posición de la letra *b* en la tabla). Continuamos:

$$C(\text{a}) = 0 + 3 \pmod{26} = 3 \pmod{26} = 3,$$

y sustituimos la letra *a* por la *D*, ya que la letra *d* ocupa la posición 3 en la tabla... Y así sucesivamente, con el resto de las letras, de manera que resulta el criptograma:

BDYLYHRFXOWD

Para desencriptarlo, basta con usar la fórmula inversa:

$$D(x) = x - 3 \pmod{26},$$

donde, si resulta un número negativo, se le suma 26. Aplicándola letra a letra al criptograma:

$$D(\text{B}) = 1 - 3 \pmod{26} = -2 \pmod{26} = 24 \pmod{26} = 24,$$

luego desciframos la letra *y* (ya que –2 es negativo, se suma 26, obteniendo 24, que es la posición de la letra *y* en la tabla); etc.

De modo más general, podemos hacer uso de distintas ordenaciones de las diferentes letras del alfabeto. Hay $26! = 26 \cdot 25 \cdot \ldots \cdot 3 \cdot 2 \cdot 1$ maneras distintas de ordenar 26 caracteres —sus permutaciones—, un número muy grande (del orden de 10^{26}), lo cual quiere decir que son posibles 26! tablas diferentes de sustitución. Ello ofrece una nueva posibilidad, mucho más segura, de

ARITMÉTICA MODULAR

Recordemos que el sistema binario es de base dos, lo que quiere decir que maneja solo dos caracteres o bits, el 0 y el 1 (el sistema decimal emplea diez, del 0 al 9). Un número natural x en un sistema binario de N bits se representa como una hilera de N ceros y unos, $(n_{N-1}, n_{N-2}, \ldots, n_2, n_1, n_0)$, teniéndose que:

$$x = n_{N-1} \cdot 2^{N-1} + n_{N-2} \cdot 2^{N-2} + \ldots + n_2 \cdot 2^2 + n_1 \cdot 2^1 + n_0 \cdot 2^0.$$

Un cifrado César binario utiliza un alfabeto de solo dos letras o caracteres, 0 y 1, de forma que hay que aplicar el módulo 2 en la correspondiente fórmula de sustitución por desplazamiento de tres posiciones. Es decir, se tendría la fórmula:

$$C(x) = x + 3 \pmod 2.$$

De acuerdo con ella, la palabra «oculta», por ejemplo, se cifraría como el criptograma 111001, ya que:

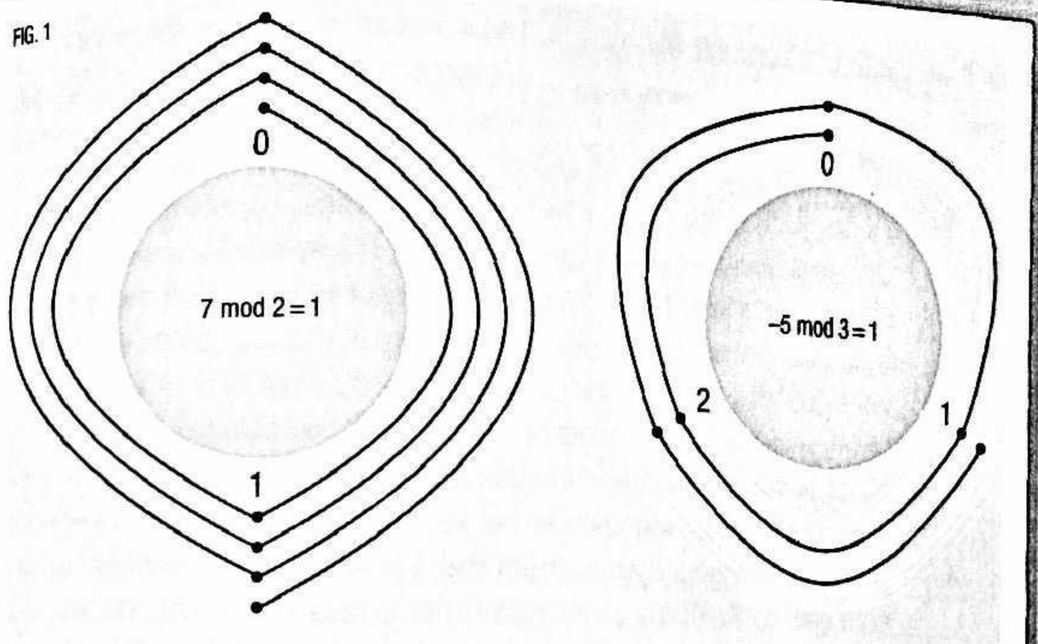
C(o) = 14 + 3 (mod 2) = 17 (mod 2): carácter 1;
C(c) = 2 + 3 (mod 2) = 5 (mod 2): carácter 1;
C(u) = 20 + 3 (mod 2) = 23 (mod 2): carácter 1;
C(l) = 11 + 3 (mod 2) = 14 (mod 2): carácter 0;
C(t) = 19 + 3 (mod 2) = 22 (mod 2): carácter 0;
C(a) = 0 + 3 (mod 2) = 3 (mod 2): carácter 1.

Podemos imaginar el reloj del esquema izquierdo de la figura 1, con solo dos números, 0 y 1, y tomar el mod 2 de cualquier número entero positivo n de la siguiente manera: empezando a partir de la posición 0, realizar la secuencia horaria de movimientos $0 \to 1 \to 0 \to \ldots$, dando n pasos o saltos; la posición final, bien 0, bien 1, nos indicará el valor de n (mod 2). Por ejemplo, utilizando la figura, se obtiene 7 (mod 2) = 1. Para calcular con otros módulos, se puede usar el mismo procedimiento. Por ejemplo, en módulo 8 pondríamos ocho horas o posiciones en el reloj, numeradas de 0 a 7, e iríamos saltando sucesivamente de una a otra. Por ejemplo, 9 (mod 8) = 1 (ya que $9 = 8 \cdot 1 + 1$, con un residuo de $1 = 9 - 8$ en la correspondiente división de 9 entre 8 para dar 1); 14 (mod 8) = 6 (ya que $14 = 8 \cdot 1 + 6$, con residuo $6 = 14 - 8$ en la división de 14 entre 8 para dar 1); etc. Para un número entero negativo, daríamos los pasos en sentido antihorario, como se muestra a la derecha en la figura.

Matemática de módulo 2 y la operación lógica XOR

En la aritmética de módulo 2, simplemente se ignoran los acarreos, de forma que la suma y la resta binarias en módulo 2 se igualan a la operación lógica denominada XOR, cuya tabla de verdad, es decir, el valor de la suma en módulo 2 de dos bits, se muestra en la figura 2, junto con un ejemplo de suma y resta en módulo 2 de tres bits. La puerta lógica XOR, o disyunción exclusiva lógica, se corresponde con la suma aritmética binaria de módulo 2; su símbolo como operador es $\oplus$ y realiza la función booleana $A \oplus B = A'B + AB'$, donde la prima (') simboliza la negación, y +, la disyunción no exclusiva (OR).

FIG. 1



Representaciones del procedimiento para calcular el módulo de un número entero positivo (izquierda) y negativo (derecha).

FIG. 2

A	B	A XOR B
0	0	0
0	1	1
1	0	1
1	1	0

$$\begin{array}{r} 1\ 0\ 1 \\ +\ 0\ 1\ 1 \\ \hline 1\ 1\ 0 \end{array} \qquad \begin{array}{r} 1\ 0\ 1 \\ -\ 0\ 1\ 1 \\ \hline 1\ 1\ 0 \end{array}$$

Tabla de verdad XOR y ejemplo de suma y resta de tres bits en módulo 2.

cifrado: escoger al azar una cualquiera de esas 26! permutaciones; su lectura exigirá entonces conocer cuál se ha empleado y aplicar la permutación inversa. Dado el gran número de posibilidades, en principio podría parecer que el criptoanálisis del cifrado sería casi imposible. Pero, de la mano del matemático Al-Kindi, autor en el siglo IX de un tratado de criptoanálisis, el análisis de frecuencias proporcionó un eficaz método de desencriptado para estos sistemas de sustitución. Como explica Edgar Allan Poe en su cuento *El escarabajo de oro*, si se incorporan las características específicas de la lengua que se está usando, tales como las frecuencias de aparición de las distintas letras, y las apariciones obligadas de algunas letras seguidas, puede romperse el cifrado, siempre que el texto tenga una longitud suficiente. Como datos de muestra, en español (un alfabeto de módulo 27) las letras más frecuentes son la *e* y la *a*, con frecuencias respectivas del 13-16% y del 10-12%, dependiendo del sistema de medición, mientras que las seis menos frecuentes son las letras *k*, *w*, *x*, *ñ*, *j* y *z*, que no suelen ocupar en conjunto más del 1-3% de cualquier texto, mientras que artículos y preposiciones como *el*, *la*, *de*, *en*, etc., ocuparán alrededor del 30%. Además, se presentan dígrafos cuya frecuencia también se conoce, por ejemplo, sabemos que la *q* va siempre seguida de la *u*.

El que confía sus secretos a otro hombre se hace esclavo de él.

BALTASAR GRACIÁN

Para resistir mejor el criptoanálisis del método de las frecuencias, se desarrollaron los cifrados que recurrían a más de un alfabeto. En el siglo XV, Leon Alberti no solo usó varios alfabetos de cifrado, para distintas partes de un mismo mensaje, sino que, además, ideó un sistema de discos móviles que hacían posible un eficaz uso de este sistema de sustitución polialfabética. Se trató, probablemente, del primer mecanismo automático de cifrado de una larga serie, que culminaría en el siglo XX con las máquinas cifradoras electromecánicas a rotor, indispensables para los diferentes servicios secretos. Entre ellas pueden citarse las populares Enigma y Lorenz (Alemania); Sigaba (Estados Unidos), de funcionamiento similar al de Enigma, y Purple (Japón).

*En el siglo XVI nació un sistema de criptografía por sustitución polialfabética muy conocido, el sistema de cifrado Vigenère, método que, por ejemplo, puede ejecutarse haciendo uso de una clave preacordada y un *cuadrado de Tritemio*, una tabla en la que se muestran todos los alfabetos de sustitución o claves que se van a emplear. La figura 1 muestra el correspondiente cuadrado para el alfabeto latino moderno (26 claves).*

FIG. 1

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
a	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
b	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
c	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
d	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
e	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
f	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
g	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
h	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
i	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
j	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
k	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
l	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
m	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
n	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
o	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
p	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
r	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
s	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
t	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
u	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
v	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
w	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
x	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

Cuadrado de Tritemio de 26 claves, útil para implementar, por ejemplo, un cifrado Vigenère.

Una vez acordada la palabra clave, por ejemplo, *VIVEOCULTO*, se procede a escribirla repetitivamente debajo del mensaje que se desea codificar, en este ejemplo «líbrate de la rutina»:

l	i	b	r	a	t	e	d	e	l	a	r	u	t	i	n	a
V	I	V	E	O	C	U	L	T	O	V	I	V	E	O	C	U

A continuación, se procede al cifrado utilizando el cuadrado de Tritemio, siendo posibles distintos métodos; por ejemplo, en un cifrado Vigenère los pares de letras alineados en columna en esta tabla constituyen las coordenadas de la letra que va a sustituir a la correspondiente del mensaje, siendo indiferente su orden. Así, el mensaje y la clave anteriores definen una serie de coordenadas: (l, V), (i, I), (b, V)... Usando el cuadrado de Tritemio, podemos obtener el criptograma (tomamos la primera coordenada como fila y la segunda como columna):

GQWVOVYOXZVZPXWPU

Estos tipos de cifrados polialfabéticos fueron considerados inviolables, ya que al usar símbolos distintos para una misma letra se consiguen frecuencias de aparición más homogéneas, tanto más cuanto más larga sea la clave, por lo que el cifrado es inmune al análisis de frecuencias. Parecía, pues, que el secreto de la clave garantizaba la confidencialidad del mensaje, y así se creyó durante mucho tiempo, hasta que, a mediados del siglo XIX, Charles Babbage logró romper este tipo de cifrado, con un método publicado poco después por Friedrich Kasiski y que conseguía una gran tasa de éxito. Esencialmente, el criptoanálisis se centra en averiguar la longitud de la clave usada, a partir de la localización y análisis estadístico de grupos de tres o más símbolos seguidos que se repitan en el criptograma, lo cual suele indicar casi siempre que dichas palabras eran la misma antes del cifrado y que la clave coincidió en la misma posición en ambas ocurrencias. Sabiendo entonces que la distancia entre palabras repetidas es un múltiplo de la longitud de la clave, se busca el máximo común divisor entre las distintas distancias así localizadas. La longitud de la clave será este número o algún factor primo del mismo; a partir de ese dato, se consigue romper el cifrado, mediante un complicado proceso de análisis de frecuencias que permite averiguar la clave. En 1922, William Friedman desarrollaría otro método de violación para este cifrado, complementario al de Kasiski, a partir de la introducción de los *índices de coincidencia* o probabilidades de que se repitan dos símbolos sacados al azar del criptograma, lo que supuso una temprana ligadura de la matemática y la estadística con la criptología.

Por lo expuesto, está claro que la principal debilidad de estos cifrados es la naturaleza repetitiva de su clave. En 1918, Gilbert Vernam declaró que solo serían inviolables si se utilizase una clave generada completamente al azar, para evitar las peculiaridades de cada lenguaje natural, y como mínimo tan larga como el texto o mensaje a encriptar. Como es fácil imaginar, usar claves tan largas no resulta muy práctico.

El secreto perfecto

Claude Shannon demostró matemáticamente en 1949, en su trabajo «Teoría de las comunicaciones secretas», que el cifrado Vernam es, en efecto, inviolable, pero a condición de que la clave sea de igual longitud que el texto a cifrar y se utilice solo una vez, un proceder que se encuadra en un tipo de sistemas criptográficos que se denominan *de libreta de un solo uso* (en inglés, *one-time-pad*). Lograr lo que Shannon definió como «secreto perfecto», o mensaje cuyo cifrado es seguro frente a un criptoanálisis con tiempo y recursos ilimitados, ya que el criptograma no proporciona absolutamente ninguna información acerca del texto original, requiere, pues, el uso de un gran cuaderno secreto de claves, del que se tiene que usar una «página» o clave distinta cada vez, destruyéndola a continuación (algo que resulta engorroso y complicado). A partir de las últimas décadas del siglo XX, se propusieron muchos sistemas criptográficos de clave

EL IMBATIBLE CIFRADO VERNAM DIGITAL

Un cifrado Vernam puede implementarse digitalmente, haciendo uso de la operación aritmética suma con módulo 2. Si queremos seguridad total, en este cifrado la clave debe ser una secuencia binaria aleatoria de la misma longitud —número de bits— que el texto plano.

Cifrando con ASCII y XOR

Por ejemplo, vamos a cifrar la palabra «razón». Primero la escribimos en binario, haciendo uso del código ASCII (*American Standard Code for Information Interchange*, Código Estándar Estadounidense para el Intercambio de Información) de representación de caracteres, parte del cual se muestra en la tabla de la página contigua. Este código establece una correspondencia entre diversos símbolos y los números decimales del 0 al 127, representables en binario con un conjunto de siete bits ($2^7 = 128$), lo que permite su procesado en dispositivos digitales. Así, podemos escribir *razon* como: 114-97-122-111-110; a continuación, escribimos cada uno de estos números en binario: 1110010-1100001-1111010-1101111-1101110. Después creamos una clave aleatoria de igual longitud, por ejemplo, *TVHLB*, con la que procedemos como se indica en la tabla de abajo. Sumamos en módulo 2 —operación lógica XOR— los números binarios en cada columna y empleamos de nuevo su conversión ASCII, lo que produce finalmente el criptograma: &-7-2-#-,. Para recuperar el mensaje original, basta con sumar al criptograma la clave, obteniéndose así la fila (4), que coincide con la (3), ya que adición y sustracción coinciden en la aritmética de módulo 2. La tabla bajo estas líneas ilustra todos los pasos.

Texto plano		r	a	z	o	n
	ASCII	114	97	122	111	110
(1)	Binario	1110010	1100001	1111010	1101111	1101110
	CLAVE	T	V	H	L	B
	ASCII	84	86	72	76	66
(2)	Binario	1010100	1010110	1001000	1001100	1000010
(3) = (1) ⊕ (2)	Suma mod 2	0100110	0110111	0110010	0100011	0101100
	Decimal	38	55	50	35	44
Criptograma	ASCII	&	7	2	#	,
(4) = (1) = (3) ⊕ (2)	Suma mod 2	1110010	1100001	1111010	1101111	1101110

Byte	Código	Carácter	Byte	Código	Carácter	Byte	Código	Carácter
00100000	32	Espacio	01000000	64	@	01100000	96	`
00100001	33	!	01000001	65	A	01100001	97	a
00100010	34	"	01000010	66	B	01100010	98	b
00100011	35	#	01000011	67	C	01100011	99	c
00100100	36		01000100	68	D	01100101	100	d
00100101	37	%	01000101	69	E	01100101	101	e
00100110	38	&	01000110	70	F	01100110	102	f
00100111	39	'	01000111	71	G	01100111	103	g
00101000	40	(	01001000	72	H	01101000	104	h
00101001	41	)	01001000	73	I	01101001	105	i
00101010	42	*	01001010	74	J	01101010	106	j
00101011	43	+	01001011	75	K	01101011	107	k
00101100	44	,	01001100	76	L	01101100	108	l
00101101	45	-	01001101	77	M	01101101	109	m
00101101	46	.	01001110	78	N	01101110	110	n
00101111	47	/	01001111	79	O	01101111	111	o
00110000	48	0	01010000	80	P	01110000	112	p
00110001	49	1	01010001	81	Q	01110001	113	q
00110010	50	2	01010010	82	R	01110010	114	r
00110011	51	3	01010011	83	S	01110011	115	s
00110100	52	4	01010100	84	T	01110100	116	t
00110101	53	5	01010101	85	U	01110101	117	u
00110110	54	6	01010110	86	V	01110110	118	v
00110111	55	7	01010111	87	W	01110111	119	w
00111000	56	8	01011000	88	X	01111000	120	x
00111001	57	9	01011001	89	Y	01111001	121	y
00111010	58	:	01011010	90	Z	01111010	122	z
00111011	59	;	01011011	91	[	01111011	123	{
00111100	60	<	01011100	92	\	01111100	124	|
00111101	61	=	01011101	93	]	01111101	125	}
00111110	62	>	01011110	94	^	01111110	126	~
00111111	63	?	01011111	95	_	01111111	127	Supr

Tabla estándar (parcial) de códigos US-ASCII. En la primera columna se indica el correspondiente byte (conjunto de 8 bits) para cada código. El primer bit es siempre nulo y se usaba originariamente como recurso de control; posteriormente, al ampliarse la tabla a 256 códigos, se incorporó también a la representación de los distintos caracteres.

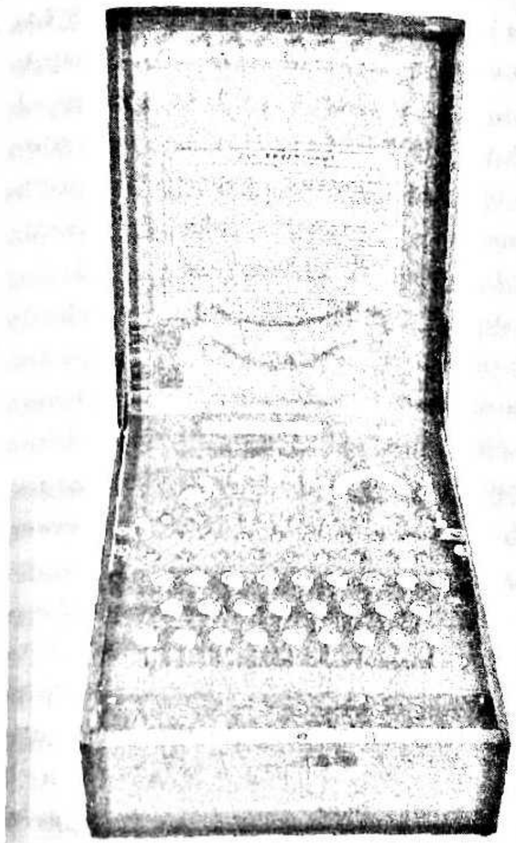
privada —también denominados simétricos, en los que los interlocutores comparten una clave secreta—, más prácticos que el Vernam porque usaban claves reutilizables y más breves que el mensaje que se quería cifrar. Aunque algunos de ellos permanecen todavía sin ser violados, tampoco se ha logrado establecer matemáticamente su invulnerabilidad.

Tres pueden guardar un secreto
si dos de ellos están muertos.

BENJAMIN FRANKLIN

La historia ofrece muchos ejemplos de métodos más ingeniosos de criptografía clásica, hoy englobados, con sus correspondientes métodos de criptoanálisis, bajo la denominación usual de criptología precientífica, algunos de los cuales jugaron un papel decisivo en hechos históricos fundamentales, como las guerras. Un ejemplo es la hoy muy popular y antes mencionada máquina de cifrado Enigma, usada por los alemanes en la Segunda Guerra Mundial (véase las fotografías superiores de la página contigua). Las claves de los criptogramas que producía se lograron averiguar gracias a un equipo de investigadores liderado por Max Newman y uno de los padres de la informática y de la inteligencia artificial, Alan Turing (en la página contigua, abajo). Esta primera etapa se suele considerar que se extiende hasta mediados del siglo XX, cuando Shannon, uno de los fundadores de la teoría de la información, desarrolló la fundamentación matemática de la criptografía, sugiriendo utilizar operaciones múltiples que mezclaran transposiciones y sustituciones y marcando con ello el inicio de la etapa científica de la criptología.

A partir de entonces, el desarrollo de la informática y los avances matemáticos permitieron que los nuevos algoritmos de cifrado fueran cada día más complejos y eficaces. En 1973, los organismos oficiales estadounidenses hicieron una convocatoria pública para promover nuevos sistemas criptográficos, fruto de la cual se desarrolló el complejo sistema DES (*Data Encryption Standard*, estándar de cifrado de datos), presentado por la compañía IBM dos años después. Se trata de un sistema de cifrado simétrico, de clave secreta o privada, que opera sobre bloques de datos de 64 bits y utiliza una clave de 56 bits. Adop-



La máquina Enigma (arriba a la izquierda), un hito de la criptografía clásica, jugó un papel esencial en la Segunda Guerra Mundial, al usarse para encriptar las comunicaciones del ejército alemán (derecha). Junto a estas líneas, escultura de Alan Turing realizada por Stephen Kettle. El matemático desarrolló una estrategia para romper los códigos Enigma, diseñando la máquina electromecánica Bombe.

tado por muchos países, fue finalmente descifrado en varios ataques distintos, el definitivo en 1998, en un tiempo récord de 56 horas por medio de un ataque de simple «fuerza bruta», o búsqueda exhaustiva de la clave probando una tras otra, algo que, por supuesto, involucra ingentes recursos informáticos. De modo que se convocó otro concurso, que promovió el desarrollo de su sucesor, AES (*Advanced Encryption Standard*, estándar de cifrado avanzado), cuyos creadores fueron Joan Daemen y Vincent Rijmen. Se trata también de un cifrado simétrico, pero opera sobre bloques de datos mayores que el DES y con longitudes de clave hoy en día de cientos o miles de bits. Fue adoptado oficialmente en 2002 y, sometido a criptoanálisis continuo desde entonces, ninguno de los ataques exitosos publicados se considera todavía lo suficientemente eficaz como para considerarlo realmente *quebrado*, lo que en criptoanálisis significa que se puede romper con un método más rápido que la simple fuerza bruta. Pero en su horizonte acecha la amenaza de la computación cuántica y sus algoritmos, como el de Grover, que optimiza la búsqueda de un dato en una lista o secuencia de N elementos, el tipo de proceso que se necesita implementar para romper la seguridad de cifrados como los DES y AES.

Debe considerarse que, si bien en sus primeros usos un algoritmo de cifrado puede suponerse desconocido, con el tiempo se difundirá, de modo que la seguridad de un cifrado no puede depender de la mayor o menor difusión del algoritmo usado, sino que debe radicar en el secreto de la clave y, en caso de ser interceptada, de su fortaleza frente al criptoanálisis, de manera que con frecuencia una clave se usa para cifrar otras, en una jerarquía progresiva. Mientras que todos los sistemas hasta 1976 eran simétricos, haciendo uso de claves que han de mantenerse como un secreto adicional al del mensaje entre emisor y receptor, ese año Whitfield Diffie y Martin Hellman propusieron en su trabajo «Nuevas direcciones en criptografía» desarrollar sistemas criptográficos asimétricos, idea novedosa a la que también contribuyeron Ralph Merkle y Clifford Cocks. La idea consiste en añadir a la clave privada una clave pública. Conocidos como sistemas CSCP (criptosistemas de clave pública), uno de los primeros fue el RSA (por las iniciales de sus creadores, Ron Rivest, Adi Shamir y Leonard Adleman), publicado en 1977 y considerado muy seguro, pero de elevada complejidad y gran coste asociados, por lo que suele utilizarse solo para temas trascendentales (como, por ejemplo, la generación de firmas digitales). En un sistema asimétrico de cifrado se emplean dos claves por usuario, una privada y otra pública; su ventaja es que no se requiere intercambiar clave alguna. Por ejemplo, en RSA, cada usuario posee sus claves propias de cifrado, la pública y la privada, generadas a partir de una determinada pareja de números primos grandes, elegidos por él y que constituyen un secreto que debe preservar con celo. Imaginemos dos amigos, Alicia y Blas, que quieren disponer de un canal de información mutuo secreto vía RSA. Si, por ejemplo, Alicia desea enviar un mensaje a Blas, busca la clave pública de él, cifra su mensaje con esa clave, y cuando Blas reciba ese criptograma así generado, lo descifrará usando su (de él) clave privada. Por tanto, no realizan ningún intercambio de claves, y está garantizado que solo Blas podrá descifrar el mensaje, ya que él ha generado sus dos claves a partir de su pareja secreta de números primos, mediante operaciones matemáticas muy complejas que involucran funciones *de un solo sentido*, fáciles de calcular en una dirección pero muy difíciles de invertir (algoritmo cuántico de Grover al margen), sobre todo cuando los factores primos involucrados son distintos, muy grandes y de tamaño similar.

El criptoanálisis de los métodos asimétricos ha establecido, pues, que su seguridad, suponiendo que se use una clave pública lo suficientemente larga, depende, en última instancia y esencialmente, de cuán rápido y eficaz pueda resolverse el problema matemático de la descomposición de un número grande en factores primos (un teorema fundamental de la aritmética establece que cualquier entero mayor que 1 puede escribirse de forma única como un producto de números primos). En consecuencia, protocolos como el RSA podrán considerarse seguros mientras que no se conozcan algoritmos eficaces para abordar esa tarea de descomposición. Sin embargo, desde la publicación en 1994 del algoritmo de Shor para la factorización de números

grandes en factores primos, se piensa que se cierne sobre la seguridad del cifrado RSA una seria amenaza teórica. Pero como su aplicación requiere un ordenador cuántico operativo con una memoria estable de un tamaño que todavía está muy lejos de alcanzarse, hoy por hoy el algoritmo RSA sigue siendo seguro en la práctica, ya que la factorización en números primos sigue siendo inabordable para los computadores clásicos, al menos en tiempos sensatos. De hecho, aunque se han publicado rupturas para claves por debajo de los mil bits, conseguidas con muchas horas de computación en miles de ordenadores cooperando en sus horas libres a lo largo del mundo —la compañía RSA ofrece golosos premios para los que consigan tales éxitos criptoanalíticos—, el descifrado de claves de unos 2000 a 4000 bits, como las que se usan hoy en las altas instancias, se supone imposible, pues se cree que conllevaría millones de años de proceso. Ahora bien, seamos prudentes, siempre cabe pensar que se podrían ir desarrollando mejores algoritmos de factorización implementables en ordenadores clásicos, que van también siendo de manera progresiva mucho más potentes.

El problema de la gestión de claves y la interceptación

No olvidemos que siempre cabe la posibilidad de acceder a las claves mediante el espionaje. Sorprendentemente, en 2013 unos investigadores israelíes —Daniel Genkin, Eran Tromer y el propio Shamir, uno de los inventores del RSA— publicaron un artículo en el que explicaban cómo habían logrado hacerse con la clave de un tipo de cifrado RSA por medio de un criptoanálisis acústico: analizando los sonidos emitidos por la CPU de varios modelos de ordenador durante el descifrado de algunos criptogramas seleccionados. Este tipo de ataques, denominados *ataques de canal lateral*, miden en general el consumo de energía en el ordenador cuando va realizando los distintos cálculos matemáticos del algoritmo. Existen otros muchos tipos de ataques, como los denominados *de cifrado cíclico*, en los que un criptograma interceptado se va recifrando sucesivamente con la correspondiente clave pública con que se generó, hasta que se logra romper el código (algo extremadamente complicado para claves lo bastante grandes).

Es obvio que para la seguridad de todos los cifrados simétricos es muy importante el sistema de intercambio de claves que se adopte. En cambio, podría pensarse que en un sistema asimétrico la buena gestión de claves ya no va a ser crucial, puesto que no se intercambia clave alguna. Sin embargo, no es así, el problema de cómo gestionar y distribuir las claves subsiste, siendo crucial para la seguridad establecer cómo se acreditan los intervinientes en un intercambio de información, ante la posibilidad de sufrir una interceptación y, a continuación, un ataque del tipo denominado *de falsa respuesta*, con suplantación de identidad. Veamos en qué consisten con un ejemplo. Supongamos que Eva, nuestra espía, quiere interceptar la comunicación entre Alicia y Blas, y consigue publicar una clave de un modo que hace que Alicia la interprete erróneamente como la clave pública de Blas (y confunde de manera análoga a Blas, proporcionándole una falsa clave como la pública de Alicia). Si Eva es capaz de interceptar los criptogramas que Alicia envía a Blas, por ejemplo, además de leerlos sin problemas —puesto que están generados con una clave suya y no con la pública de Blas, de modo que solo tiene que aplicarle su (de Eva) clave privada—, también puede ocultar su espionaje, enviándole a Alicia un criptograma con la respuesta de Blas, pero espurio, elaborado por ella a partir de la verdadera clave pública de Alicia, por lo que esta lo descifrará sin problemas y sin advertir el espionaje. Eva hace lo mismo con los mensajes de Blas hacia Alicia, de modo que ninguno de los dos tiene por qué darse cuenta de que están siendo espiados. Es decir, Alicia y Blas creen que se están comunicando en secreto, pero en realidad sus mensajes están siendo espiados por Eva, sin que ellos se den cuenta. Es contra este tipo de ataques contra los que se desarrollaron los certificados de firma digital, que acreditan la autenticidad de los emisores de un mensaje mediante la intervención de una «autoridad de certificación», que garantiza que la correspondiente clave pública pertenece realmente a la persona con la que se quiere comunicar.

La cuestión de la gestión de claves fue el entorno teórico en que se produjo la primera propuesta de aplicación de la física cuántica a la criptología. Se trata del protocolo BB84, que describiremos más adelante, tras una pequeña introducción a la criptología cuántica.

LA CRIPTOGRAFÍA CUÁNTICA

Después del breve recorrido hecho por la criptografía clásica, parece claro que presenta dos problemas. Por un lado, el hecho de que la seguridad completa, aunque demostrada matemáticamente como posible para un cifrado simétrico con clave totalmente aleatoria —algo difícil de garantizar—, de un solo uso y tan larga como el mensaje que se desea cifrar, resulta tan complicada de implementar que es poco práctica, además de requerir el intercambio de la clave secreta compartida, un proceso siempre abierto a un posible espionaje indetectable. Por otro lado, los sistemas de clave pública o asimétrica, que eliminan la necesidad de compartir una clave y, por tanto, de distribuirla, aparte de que no se haya establecido matemáticamente su seguridad completa, plantean el problema de la suplantación de identidades en la comunicación. Pues bien, vamos a ver cómo la aplicación de la física cuántica a la criptología elimina algunos de estos obstáculos, puesto que hace posible métodos seguros de generación y distribución de claves que, aunque siguen consistiendo en secuencias aleatorias de bits clásicos, se van a generar a partir de qubits, los bits cuánticos. Se garantiza así que cualquier vulneración de la seguridad o espionaje que se produzca será irremediablemente detectado, gracias a la acción de los principios cuánticos.

El origen de la criptografía cuántica suele asociarse con Stephen Wiesner, quien, en la década de 1960, concibió la idea de aplicar las relaciones de indeterminación que ligan las propiedades físicas complementarias de un sistema cuántico a propósitos como, por ejemplo, conseguir billetes imposibles de falsificar. Sus ideas sonaron tan extravagantes por aquel entonces que no logró publicarlas hasta 1970. De hecho, no sería hasta los años ochenta cuando estos temas empezaron a considerarse en serio, de manera que Charles Bennett y Gilles Brassard, ambos de IBM, iniciaron un trabajo que daría como fruto el famoso protocolo BB84, una aplicación cuántica a la criptografía de clave secreta que implementa un protocolo seguro de distribución de clave o, en jerga criptológica, mecanismo de QKD (*Quantum Key Distribution*, distribución de claves cuánticas), con el que cualquier interceptación del mensaje por terceros será detectada por los interlocutores.

El protocolo BB84

En criptografía cuántica, los bits clásicos de la clave se van a generar e intercambiar mediante qubits. Conviene recordar que estos corresponden matemáticamente al estado general de superposición o suma de dos estados cuánticos básicos, 0^q y 1^q, los análogos de los bits clásicos 0 y 1:

$$\Psi = a \cdot 0^q + b \cdot 1^q;$$

los números a y b —sus módulos al cuadrado— representan las probabilidades de que, al forzar mediante un experimento de medida a que el sistema abandone la superposición, quede como resultado final en uno de esos dos estados que se combinan en Ψ. Este qubit abstracto se puede implementar físicamente de muchas maneras, por ejemplo, sobre fotones, disponiéndolos en un estado de superposición de dos polarizaciones distintas fundamentales.

La idea en la que se basa el protocolo cuántico BB84 es conjugar el envío de un mensaje por un canal tradicional o clásico con un envío adicional, por un canal cuántico, de una serie de qubits, implementados sobre fotones en distintos estados cuánticos de polarización. De esta manera, dos comunicantes —nuestros Alicia y Blas— se van a intercambiar una clave secreta aleatoria, escrita sobre fotones, que luego se supone que usarán para cifrar sus comunicaciones con un cifrado clásico como, por ejemplo, el Vernam. La seguridad que conlleva la incorporación del canal

cuántico va a ser que, en virtud del principio de indeterminación y el colapso cuántico, si cualquier espía —nuestra Eva— intercepta el canal cuántico —los fotones con los que se va a generar la clave secreta—, inapelablemente dejará una huella de su acción que será detectada por Alicia y Blas, quienes entonces desecharán esa clave.

Comencemos el protocolo. Alicia, por ejemplo, envía a Blas una radiación compuesta por una serie de pulsos monofotónicos sucesivos, que han sido forzados a determinar su estado de polarización superpuesto inicial,

$$\psi = 1/\sqrt{2}\cdot 0^{o} + 1/\sqrt{2}\cdot 1^{o},$$

hacia una de entre las cuatro posibilidades →, ↑, ↗ o ↘. Para conseguirlo, basta, por ejemplo, con hacer pasar muchos fotones despolarizados por un cristal de calcita orientado en modo recto: la mitad de los fotones que lo atraviesen quedarán a la salida del cristal en el estado ↑, y la otra mitad, en el estado →. En cambio, si la calcita se hubiera orientado en modo diagonal, la mitad de los fotones habría resultado ↗ y los restantes, ↘. De manera que, para conseguir una secuencia aleatoria de polarizaciones, basta con disponer de un haz de luz compuesto por pulsos monofotónicos que inciden sobre un cristal de calcita, y elegir para cada uno de ellos, al azar, uno de los dos modos de orientación de la calcita, recto (R) o diagonal (D). Alicia codifica así sobre los fotones una serie de qubits colapsados, esto es, que han sido determinados a una polarización concreta desde la superpuesta inicial. Por ejemplo, consideremos que Alicia genera la siguiente secuencia, que suponemos determinada por completo al azar:

Orden del fotón	1	2	3	4	5	6	7	8	9	10	...
Modo calcita (al azar)	R	D	D	D	R	R	D	R	D	R	...
Estado final de polarización	→	↗	↘	↗	↑	↑	↗	→	↘	↑	...
Qubit	0^o	0^o	1^o	0^o	1^o	1^o	0^o	0^o	1^o	1^o	...

La serie de fotones es transmitida a continuación, por ejemplo por una fibra óptica, y le va llegando a Blas, que entonces, de nuevo al azar, decide si va a hacer pasar cada fotón por un analizador —un cristal de calcita— orientado en modo recto o en modo diagonal. La tabla siguiente resume todos los posibles resultados que obtendría sobre cada fotón entrante, para cada una de las dos elecciones de orientación de su calcita que puede hacer:

Polarización a la entrada	Qubit entrante	Modo calcita Blas (al azar)	Resultado	Qubit leído	Ratio coincidencias
→	0^o	R	→100%	0^o 100%	100%
→	0^o	D	↗50%, ↘50%	0^o 50%, 1^o 50%	50%
↑	1^o	R	↑100%	1^o 100%	100%
↑	1^o	D	↗50%, ↘50%	0^o 50%, 1^o 50%	50%
↗	0^o	R	→50%, ↑50%	0^o 50%, 1^o 50%	50%
↗	0^o	D	↗100%	0^o 100%	100%
↘	1^o	R	→50%, ↑50%	0^o 50%, 1^o 50%	50%
↘	1^o	D	↘100%	1^o 100%	100%

A continuación, aplicamos esta tabla de resultados sobre la serie de diez fotones que suponemos que le envía Alicia:

Orden del fotón	1	2	3	4	5	6	7	8	9	10	...
Modo calcita Alicia (azar)	R	D	D	D	R	R	D	R	D	R	...
Resultado Alicia	→	↗	↘	↗	↑	↑	↗	→	↘	↑	...
Qubits enviados	0^o	0^o	1^o	0^o	1^o	1^o	0^o	0^o	1^o	1^o	...
Modo calcita Blas (azar)	R	D	R	R	R	R	D	D	D	D	...
Qubits leídos	0^o	0^o	0^o o 1^o	0^o o 1^o	1^o	1^o	0^o	0^o o 1^o	1^o	0^o o 1^o	...
Ratio coincidencias	100%	100%	50%	50%	100%	100%	100%	50%	100%	50%	...
Bits clave	0	0	—	—	1	1	0	—	1	—	...

Es ahora cuando interviene el canal clásico. Blas informa a Alicia —por teléfono, correo, etc.— de la secuencia de orientaciones de la calcita que eligió para sus medidas, y Alicia responde por el mismo canal indicándole en qué fotones —columnas en la tabla— los modos coinciden. En el ejemplo, han coincidido en los fotones 1, 2, 5, 6, 7 y 9, cuyas columnas se hallan sombreadas (en promedio, coincidirán un 50% de las veces, si la secuencia de fotones es lo suficientemente larga). Entonces, en ese momento y sin necesidad de que intercambien ninguna información más, los dos disponen de una clave secreta común, la cadena de bits clásicos de la última fila: 001101..., que son secretos porque no han formado parte de la información que han intercambiado por el canal clásico. Pero, antes de utilizarlos como clave para cifrar sus mensajes, Alicia y Blas van a comprobar —al menos con un cierto grado de seguridad— si están siendo o no interceptados, es decir, si esa clave ha sido violada y debe ser desechada, o si pueden usarla con la confianza reforzada de que no están siendo espiados. Para ello, necesitan intercambiar información adicional por el canal clásico. En concreto, una selección de bits de la clave secreta generada, un tanto por ciento de ellos. Se ponen de acuerdo en cuáles van a ser (indicando su número de orden en la tabla) y, además, intercambian —por el mismo canal clásico— información sobre cuáles son los respectivos bits clásicos que cada uno tiene asociado con ellos. Según el procedimiento seguido, deberían coincidir todos; si no lo hacen es porque, casi con seguridad, están siendo espiados (idealmente, después rebajaremos esta expectativa porque habrá que considerar errores ajenos al espionaje). Por el contrario, si coinciden al 100% (siempre se exigirá menos, como antes, por los inevitables errores de la práctica experimental), entonces es casi seguro que no están siendo espiados, siempre que se haya tomado un grupo suficientemente grande de fotones de control. En este último caso, dado que la información sobre los bits correspondientes a esos fotones ha ido por el canal clásico, los desechan por precaución de la clave, que finalmente estará constituida solo por la secuencia de bits no controlados.

En efecto, imaginemos que Eva ha logrado acceder a la secuencia de fotones en su intento de averiguar la clave. Como Blas, tiene que hacer al azar una elección de modo de medida (orientación de la calcita) para cada fotón y, también como Blas, en promedio solo coincidirá con el que fijó Alicia en el 50% de ellos (en una secuencia suficientemente larga de fotones). En el otro 50%, fallará la mitad de las veces al leer el qubit, de modo que, en total, sobre una serie de fotones suficientemente larga, un 25% de las veces leerá un qubit que no coincide con el que Alicia envió. Además, Eva altera sin remedio estos fotones y provoca que Blas, al leerlos después, pueda asociar la mitad de las veces un bit clásico final erróneo —diferente al de Alicia—, aunque por haber coincidido con Alicia en la orientación de la calcita, no deberían haberse producido estos fallos. Si el grupo de control es suficientemente grande, incluirá con muy alta probabilidad algunos de estos fotones, y el error será detectado, por lo que Alicia y Blas sospecharán que están siendo espiados. En la tabla siguiente se muestran los resultados posibles para los mismos diez fotones de la tabla anterior, destacándose en sombreado los fotones 2, 5 y 9, sobre los que la acción de Eva ha provocado que, aunque Alicia y Blas hayan empleado la misma orientación de sus calcitas, solo haya un 50% de probabilidad de que asocien el mismo bit.

Orden del fotón	1	2	3	4	5	6	7	8	9	10
Modo calcita Alicia	R	D	D	D	R	R	D	R	D	R
Resultado Alicia	→	↗	↘	↗	↑	↑	↗	→	↘	↑
Qubits enviados	0^0	0^0	1^0	0^0	1^0	1^0	0^0	0^0	1^0	1^0
Modo calcita Eva	R	R	D	R	D	R	D	R	R	D
Resultado Eva	→	→ o ↑	↘	→ o ↑	↗ o ↘	↑	↗	→	→ o ↑	↗ o ↘
Qubits enviados	0^0	0^0 o 1^0	1^0	0^0 o 1^0	0^0 o 1^0	1^0	0^0	0^0	0^0 o 1^0	0^0 o 1^0
Modo calcita Blas	R	D	R	R	R	R	D	D	D	D
Qubits leídos	0^0	0^0 o 1^0	0^0 o 1^0	0^0 o 1^0	0^0 o 1^0	1^0	0^0	0^0 o 1^0	0^0 o 1^0	0^0 o 1^0
Ratio coincidencias Blas y Alicia	100%	50%	50%	50%	50%	100%	100%	50%	50%	50%
Bits que asocia Blas	0	0 o 1	—	—	0 o 1	1	0	—	0 o 1	—

De modo que Alicia y Blas notarán la alteración al observar que algunos de esos bits no coinciden (los que hayan entrado en el grupo de control, en el ejemplo, los bits 2, 5 y 9), y desecharán la clave completa. Como uno de cada cuatro fotones de la clave habrá sido alterado, la probabilidad de que al probar N bits se detecte el espionaje viene dada por $1-(3/4)^N$, según una estimación de Colin Williams y Scott Clearwater. En cualquier caso, este método de detección de un posible espionaje conlleva desechar bastantes fotones, por lo que se han propuesto otros métodos. Por ejemplo, sobre la selección de bits de la clave secreta generada, la que se va a usar para controlar el espionaje, en vez de comparar los bits uno a uno se puede comparar la paridad de la serie, esto es, el número de ellos que son 1; si ese número es impar, la paridad lo es, y lo mismo si es par. Para eliminar el efecto de los posibles errores de transmisión, este método habría de aplicarse siempre sobre varios subconjuntos aleatorios y no sobre uno solo. Y es que, en el caso anterior, hemos supuesto implícitamente que, por un lado, ningún fotón se perdía en la transmisión; por otro, que los polarizadores-analizadores trabajaban a la perfección, con una eficiencia del 100 %: nunca un fotón enviado como →, por ejemplo, habría salido por el canal ↑. Pero la dura realidad del laboratorio es que nunca las cosas funcionan con esa perfección ideal. Los errores —errores experimentales y errores por la decoherencia que conlleva cualquier interacción con el medio— son inevitables en la práctica, y el procesamiento cuántico de la información, por supuesto, tampoco se libra de ellos. Y es que ese qubit 0^Q que envió Alicia, durante la transmisión, antes de llegar a Blas, puede haber sufrido alguna alteración en su estado, sin que haya intervenido ninguna Eva, sino simplemente como consecuencia de cualquier interacción en su camino —en el interior de la fibra óptica, por ejemplo—. De forma que, cuando el fotón llega a Blas, la información puede haberse alterado: la decoherencia puede haberse impuesto incorporando *ruido* e, incluso, el 0^Q puede haberse convertido en un 1^Q (y viceversa). Y también, aun si ha llegado sin alteración, puede producirse un error en su lectura por el analizador. La eficiencia de un aparato nunca es del 100 %: si mandamos una serie

de fotones polarizados →, alguno siempre sale por el canal ↑, por ejemplo. Además, los detectores de radiación también yerran a veces, detectando fotones inexistentes.

En cualquier caso, el mismo método usado para detectar una posible interceptación delataría estos errores, por lo que se indicaría la necesidad de revisar por completo la forma en que se está procediendo. Se suele definir una tasa QBER *(Quantum Bit Error Rate)*, tasa de bits que, analizados sobre una parte elegida al azar de la cadena transmitida de bits de la clave, son erróneos. Para ello se transmiten y comparan por el canal clásico los valores correctos de esos bits implicados. Si la tasa QBER se mantiene inferior a un porcentaje establecido, se desecha esa parte de la cadena y el resto se toma como clave; si supera ese porcentaje, se desecha la transmisión y se vuelve a empezar. Para minimizar y corregir estos errores, se pueden adoptar diversos mecanismos. Las leyes cuánticas, como la que hace imposible la clonación de estados, requieren que sean muy diferentes a los usados en las transmisiones clásicas. Por ejemplo, como ya se comentó, no se puede pretender aplicar la redundancia o repetición de fotones producidos en el mismo estado para codificar un mismo bit. Pero esas mismas leyes proporcionan nuevos recursos: la mayoría de los métodos de corrección de errores aplicados hoy en día recurren al entrelazamiento, fenómeno que de por sí proporciona también otro protocolo de distribución de clave secreta.

El protocolo B92

En 1992 Bennett publicó un nuevo protocolo, más simple que el anterior y por eso también conocido como *protocolo mínimo*. La diferencia está en que Alicia y Blas solo van a usar uno de los dos estados de cada uno de los dos pares de estados fundamentales para enviar y leer sus qubits. Por ejemplo, Alicia elige → (qubit 0^Q) y ↘ (qubit 1^Q), de forma que va a desechar los fotones que, tras pasar cada polarizador, no resulten polarizados en uno de estos dos estados. Blas, por su parte, solo va a conservar las

lecturas que correspondan a las dos polarizaciones restantes, ↑ (qubit 1^q) y ↗ (qubit 0^q), de forma que cada uno siempre manejará un par distinto de direcciones no perpendiculares y correspondientes a distintos qubits fundamentales. La serie de fotones enviados por Alicia a Blas podría ser entonces como la siguiente (cambiaría en función del orden específico que elija Alicia para ir polarizando sus fotones, es decir, de cómo vaya orientando sucesivamente su calcita).

Orden del fotón enviado	1	2	3	4	5	6	7	8	9	10	...
Modo calcita Alicia (al azar)	R	D	D	D	R	R	D	R	D	R	...
Resultado Alicia	→	↗	↘	↗	↑	→	↘	→	↘	↑	...
Envía o no el qubit	Sí	No	Sí	No	No	Sí	Sí	Sí	Sí	No	
Qubit	0^o	—	1^o	—	—	0^o	1^o	0^o	1^o	—	...

La siguiente tabla resume todos los resultados que Blas obtendría sobre cada posible fotón entrante, para cada una de las dos elecciones de orientación de su calcita que puede hacer:

Polarización inicial	Qubit entrante	Modo calcita Blas (al azar)	Resultado	Qubit leído	Coinciden
→	0^o	R	↑: 0 %	No	—
→	0^o	D	↗: 50 %	Sí: 0^o (50 %)	Sí (ese 50 %)
↘	1^o	R	↑: 50 %	Sí: 1^o (50 %)	Sí (ese 50 %)
↘	1^o	D	↗: 0 %	No	—

Por tanto, sobre la anterior serie de fotones enviada por Alicia, Blas solo va a poder leer los fotones que aparezcan en sus ahora dos únicos canales de detección, ↑ y ↗. Es decir, cada fotón aparecerá en uno de estos dos canales solamente si llega al analizador que contiene el canal del estado no perpendicular al que él trae (y que fue determinado por la medida de Alicia). De este modo, Blas, quien decide también de forma aleatoria si los pasa por el analizador en modo recto o en modo diagonal, leería sobre cada fotón de la serie que le envía Alicia en nuestro ejemplo (columnas sombreadas en la correspondiente tabla anterior) las polarizaciones que se indican a continuación:

Orden del fotón	1	3	6	7	8	9	...
Resultado Alicia (al azar entre dos posibles)	→	↘	→	↘	→	↘	...
Qubits Alicia	0^o	1^o	0^o	1^o	0^o	1^o	...
Modo calcita Blas (al azar)	R	D	D	D	D	R	...
Probabilidad de que Blas lea el qubit	0 %	0 %	50 %	0 %	50 %	50 %	...
Qubits leídos Blas	—	—	0^o (50 %)	—	0^o (50 %)	1^o (50 %)	...
Bits clave	—	—	0 (0 —)	—	0 (0 —)	1 (0 —)	...

Es decir, es seguro que Blas no podrá leer el qubit sobre algunos fotones; para los restantes, hay una probabilidad del 50 % de que los lea. Pero cuando los lee, su lectura coincide siempre con el qubit que ha enviado Alicia. De modo que, para que los dos conozcan la clave, toda la información que hace falta transmitir por el canal clásico (del receptor al emisor) es el número de orden de los fotones que el receptor ha podido leer, nada más. A partir de ese momento, los dos comparten una clave secreta: una serie de bits clásicos (las columnas sombreadas en la última tabla).

Es obvio que en este protocolo se desaprovechan muchos más fotones que en el BB84: nada menos que las tres cuartas partes de los enviados no se usan. A cambio, el montaje es más sencillo. La detección de una posible interceptación —acción de Eva— se realiza de forma similar a como vimos antes.

Protocolo EPR o protocolo E91

Este protocolo fue propuesto por Artur Ekert en 1991 y utiliza fotones entrelazados. Por tanto, se necesita en primer lugar una fuente de pares de fotones en un estado entrelazado; de cada par habrá que hacer llegar un fotón a Alicia y otro a Blas. Supongamos que todos los pares se preparan en un estado entrelazado en el que la correlación cuántica obliga a que, medidas las polarizaciones individuales de los dos fotones con sendos cristales de calcita dispuestos con la misma orientación, los resultados coincidan siempre, al 50% para cada posibilidad.

Alicia y Blas van a proceder a pasar sus fotones por un analizador dispuesto bien en modo recto, bien en modo diagonal. Como en los anteriores protocolos, cada uno elige al azar y con independencia del otro la secuencia de orientaciones que va a seguir. En todo caso, el entrelazamiento establece que, en aquellos fotones del mismo par entrelazado en que su elección de base coincida, los resultados han de estar correlacionados; en particular, con la elección de estado entrelazado antes indicada, deben ser iguales. La tabla siguiente nos proporciona entonces un ejemplo de lo que Alicia y Blas irían encontrando al medir sobre cada fotón de los sucesivos pares entrelazados (que fueron preparados siempre en el mismo estado), y cuál sería entonces la clave secreta generada.

A la vista de la tabla, resulta claro que, cuando han elegido, por azar, la misma orientación de sus respectivas calcitas, saben que han de obtener el mismo resultado, que será 0º o 1º, pero siempre coincidente. En cambio, cuando la elección de orientación no ha sido la misma, sus qubits solamente coincidirán en el 50% de los casos. Solo necesitan informarse —por un canal clásico, que puede ser público— del orden en que cada uno ha orientado la calcita. Sobre los fotones de cada par en que han coincidido, los qubits que tienen registrados también coinciden siempre, constituyendo su clave secreta (que toman como bits clásicos). Como en los anteriores protocolos, han de incorporarse mecanismos de control de interceptación y errores.

Orden del par de fotones	Modo calcita Alicia	Resultado Alicia	Qubit leído Alicia	Modo calcita Blas	Resultado Blas	Qubit leído Blas	Las lecturas coinciden	Serie de bits de la clave común
1	R	50%: →	0º	R	50%: →	0º	Siempre	0 o 1
		50%: ↑	1º		50%: ↑	1º		
2	D	50%: ↗	0º	D	50%: ↗	0º	Siempre	0 o 1
		50%: ↘	1º		50%: ↘	1º		
3	D	50%: ↗	0º	R	50%: →	0º	50% de las veces	—
					50%: ↑	1º		
		50%: ↘	1º		50%: →	0º		
					50%: ↑	1º		
4	D	50%: ↗	0º	R	50%: →	0º	50% de las veces	—
					50%: ↑	1º		
		50%: ↘	1º		50%: →	0º		
					50%: ↑	1º		
5	R	50%: →	0º	R	50%: →	0º	Siempre	0 o 1
		50%: ↑	1º		50%: ↑	1º		
6	R	50%: →	0º	R	50%: →	0º	Siempre	0 o 1
		50%: ↑	1º		50%: ↑	1º		
7	D	50%: ↗	0º	D	50%: ↗	0º	Siempre	0 o 1
		50%: ↘	1º		50%: ↘	1º		
8	R	50%: →	0º	D	50%: ↗	0º	50% de las veces	—
					50%: ↘	1º		
		50%: ↑	1º		50%: ↗	0º		
					50%: ↘	1º		
9	D	50%: ↗	0º	D	50%: ↗	0º	Siempre	0 o 1
		50%: ↘	1º		50%: ↘	1º		
10	R	50%: →	0º	D	50%: ↗	0º	50% de las veces	—
					50%: ↘	1º		
		50%: ↑	1º		50%: ↗	0º		
					50%: ↘	1º		
...	...	...	...	...	...	...	...	...

EN LA PRÁCTICA: DISPOSITIVOS QKD OPERATIVOS Y COMERCIALIZADOS

Son muchos los problemas que se presentan a la hora de implementar en la práctica los anteriores protocolos cuánticos de distribución de claves. Uno de ellos es que la polarización no es fácil de mantener de forma estable en las transmisiones a largas distancias, ni de medir con una fiabilidad del cien por cien. Otra dificultad, no menor, es la de generar auténticos estados monofotónicos, para lo que no basta con bajar la intensidad de las fuentes de luz, procedimiento al que, sin embargo, se recurre con frecuencia. Los prototipos experimentales generalmente codifican cada qubit no en un solo fotón, sino en tenues destellos de luz, y es muy frecuente que estos consistan en más de un fotón. Esto conlleva otro agujero de seguridad: Eva podría extraer algunos de ellos, y Blas solo notaría una atenuación de la señal recibida, que atribuiría a una pérdida normal en el canal de transmisión, de manera que la acción de Eva no sería detectada. Por eso, es muy importante que los destellos se atenúen mucho, hasta un orden que garantice que solo un 1 % de los pulsos pueda contener más de un fotón. Pero, entonces, habrá algunos que se quedarán vacíos de información (sin fotones: Blas los detectará vacíos), lo que hará que la velocidad de transmisión se reduzca considerablemente. Y los protocolos, como hemos visto, requieren de largas claves, así que, por el momento, y mientras se aumenta esta velocidad, el volumen de información que se puede cifrar continuará siendo limitado frente a las posibilidades que ofrecen los métodos clásicos.

Se necesita, pues, tanto mejorar los procesos de transmisión de fotones a grandes distancias, minimizando las pérdidas en los largos tramos de fibras ópticas, como desarrollar detectores fotónicos cada vez más eficientes y con menores niveles de ruido. De cualquier forma, y como una señal clara de que las dificultades se van resolviendo, existen ya dos empresas, Id Quantique y MagiQ, que tienen a la venta dispositivos de comunicación que implementan los protocolos cuánticos de distribución de claves. Y también existen ya incipientes redes de comunicaciones cuánticas, tendidas sobre largas distancias. El ejemplo principal lo tenemos en China, que empezó a instalar en 2014 un enlace con 2 000 km de red entre Pekín y Shanghái, una iniciativa que, según se ha estimado, costará unos 100 millones de dólares, y respecto a la que Jian-Wei Pan, de la Universidad de Ciencia y Tecnología de Hefei y líder del proyecto, ha afirmado lo siguiente: «vamos a proporcionar no solo el nivel más alto de protección a los datos gubernamentales y financieros, sino que además vamos a proporcionar el mejor banco de pruebas para las teorías cuánticas y las nuevas tecnologías». El ambicioso proyecto incluía el lanzamiento de un satélite, realizado en agosto de 2016 y bautizado como QESS (*Quantum Experiments at Space Scale*, experimentos cuánticos a escala espacial), con la misión de establecer «comunicaciones cuánticas a prueba de interceptación, transmitiendo de forma segura claves entre el espacio y la superficie terrestre», según la agencia oficial de noticias china Xinhua. Es, pues, un satélite estrictamente experimental, parte de una ambiciosa investigación que cuenta con participación austriaca.

¿LA COMPUTACIÓN CUÁNTICA HARÍA IMPOSIBLE EL SECRETO PERFECTO ETERNO?

La respuesta es negativa. Incluso ante la amenaza de la futura computación cuántica, hay una posibilidad, matemáticamente establecida por Shannon, de lograr el secreto perfecto y eterno: el cifrado Vernam, con clave aleatoria de longitud igual al texto por cifrar y libreta de un solo uso (dando por supuesto que esa clave se transmite con secreto total y que la libreta se destruye a continuación). Pero, aparte de esta posibilidad, que garantiza la seguridad contra una computación de recursos infinitos, es frecuente leer que el algoritmo de Shor, unido al algoritmo de Grover y al progresivo desarrollo de la construcción de ordenadores cuánticos cada vez más grandes, nos llevará a un futuro en el que todos los algoritmos criptográficos clásicos más importantes que se usan en la actualidad estarán obsoletos. Este es, al menos, el mensaje que a veces lanzan algunos defensores y

promotores de la criptografía cuántica como única garantía real futura del secreto en las comunicaciones. Sin embargo, también son muchas las voces que señalan que se está exagerando tanto la amenaza cuántica como sus capacidades.

La mejor manera de guardar un secreto es escribir un libro.

MANUEL AZAÑA

Por un lado, en el supuesto de que llegaran los ordenadores cuánticos universales capaces de aplicar el algoritmo de Shor para números cada vez más grandes, hay que pensar que también estarían al servicio de los que cifran las comunicaciones, que podrían aumentar en la misma proporción la longitud de las claves. Es sobre esa complejidad sobre la que habría que aplicar el criptoanálisis, no sobre las longitudes de claves usadas hoy en día. Hasta la fecha, no se conoce ningún método de cifrado en tiempo polinómico que requiera un tiempo exponencial para su descifrado, pero si se llegara a desarrollar, los ordenadores cuánticos también lo tendrían difícil.

Por otra parte, como es lógico, la fortaleza de un sistema reside en su etapa más débil, que en un sistema de distribución de claves cuánticas sigue siendo la acreditación de los comunicantes, un problema distinto al de la interceptación de la comunicación en sí y que sigue sin presentar una solución práctica eficiente, aunque se han presentado ya diversos protocolos de autenticación cuántica mediante claves ópticas. Y es que Eva no puede escuchar pasivamente cómo se comunican Alicia y Blas, pero puede cortar la fibra óptica correspondiente, por ejemplo, y suplantar a los dos interlocutores, que dependerán por tanto de un mecanismo de acreditación. Además, los protocolos requieren secuencias aleatorias y, aunque existen también generadores cuánticos de números aleatorios, falta todavía investigar cómo aplicarlos de forma segura y totalmente privada a través de un canal público.

En todo caso, es evidente que un ordenador cuántico capaz de manejar el suficiente número de qubits podría realizar búsquedas de claves mediante simple fuerza bruta, a una rapidez que dejaría inservibles claves con las longitudes usadas hoy en día en los principales sistemas de criptografía considerados seguros. De modo que hay un futuro abierto y esperanzador en criptografía cuántica, que puede depararnos grandes sorpresas en cualquier momento, idealmente, un protocolo criptográfico a prueba de la misma computación cuántica, quién sabe si también seguro por completo. Ello constituiría un logro trascendental, muy diferente de los principales protocolos desarrollados y comercializados hasta la fecha, que son, sobre todo, como hemos visto, de distribución de claves.

LECTURAS RECOMENDADAS

ACZEL, A.D., *Entrelazamiento. El mayor misterio de la física*, Barcelona, Crítica, 2008.

CASSINELLO, A. Y SÁNCHEZ GÓMEZ, J.L., *La realidad cuántica*, Barcelona, Crítica, 2013.

HECHT, J.P., *Fundamentos de computación cuántica*, Madrid, Editorial Académica Española, 2012.

HERNÁNDEZ ENCINAS, L., *La criptografía*, Madrid, CSIC/Los Libros de la Catarata, 2016.

KHAN, D., *The Codebreakers: The Comprehensive History of Secret Communication from Ancient Times to the Internet*, Nueva York, Scribner, 1996.

LOEPP, S. Y WOOTTERS, W.K., *Protecting Information: From Classical Error Correction to Quantum Cryptography*, Cambridge, Cambridge University Press, 2006.

NIELSEN, M.A. Y CHUANG, I.L., *Quantum Computation and Quantum Information*, Cambridge, Cambridge University Press, 2000.

SINGH, S., *Los códigos secretos*, Barcelona, Debate, 1999.

VEDRAL, V., *Descodificando la realidad. El universo como información cuántica*, Barcelona, Biblioteca Buridán, 2011.

ÍNDICE